CCN
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 570A

IMPLEMENTACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD EN WINDOWS SERVER 2016

NOVIEMBRE 2018

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.05.08 16:39:50 +02'00'

NIPO: 083-19-032-X
Fecha de Edición: noviembre de 2018

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

PRÓLOGO

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

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

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

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

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

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

noviembre de 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE MICROSOFT WINDOWS SERVER 2016 EN EL ENS COMO CONTROLADOR DE DOMINIO O SERVIDOR MIEMBRO

ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE MICROSOFT WINDOWS SERVER 2016

1. APLICACIÓN DE MEDIDAS EN WINDOWS SERVER 2016

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación de servidores con Windows Server 2016, se establecerán, a través de la presente guía, las condiciones necesarias de aplicación. Éstas se materializarán, bien en la aplicación de plantillas de seguridad, o bien en procedimientos para garantizar la seguridad cuando así se demande. En este último caso, por ejemplo, para la segregación de roles, se detallarán procedimientos y condiciones que deberá aplicar un operador de una organización para hacerlas efectivas.

Nota: Tenga en cuenta que en el caso de una red clasificada que ha sido categorizada como Difusión Limitada se hará usó de la aplicación de medidas de seguridad descritas en el "ANEXO A.4 CATEGORÍA ALTA / DIFUSIÓN LIMITADA".

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

a) Aplicación de seguridad sobre el entorno de Directorio Activo que pueda dar soporte a la organización y sobre el que se asientan muchos de los activos tecnológicos de dicha organización. Será además el mecanismo empleado para conducir la centralización y gestión de la seguridad.

b) Aplicación de seguridad en servidores con el rol de Controladores de Dominio y que dan soporte al Directorio Activo.

c) Aplicación de seguridad en servidores miembro de dominio que sustentarán los diferentes servicios que prestara la organización, sujetos al RD 3/2010 y que se encontrarán implementados con Windows Server 2016.

Para el análisis y desarrollo de las plantillas a aplicar, así como las tareas administrativas que sean necesarias para el cumplimiento de las medidas dispuestas en el ENS, se tienen en consideración los propios elementos técnicos que aporta Microsoft para Windows Server 2016, así como otras medidas que puedan ser fácilmente aplicables mediante condiciones de seguridad válidas. Por ejemplo, todas aquellas medidas que puedan ser aplicadas a través de objetos de políticas de grupo (GPO) o las innatas a la gestión del sistema o al propio Directorio Activo, como la asignación de permisos para la segregación de roles y funciones.

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

Para un mejor entendimiento de las medidas, estás van a ser explicadas, y definidos los mecanismos que proporcione el sistema, atendiendo a los criterios de categorización. Así, se irá delimitando cada una de las medidas y estableciendo, en base a las categorías, qué mecanismos se deberán habilitar para su cumplimiento. Habida cuenta de esta información, a continuación, se detallarán las diferentes plantillas de seguridad aplicables en función de las diferentes categorías de seguridad.

1.1. MARCO OPERACIONAL

1.1.1. CONTROL DE ACCESO

El control de acceso cubre todo el conjunto de acciones que, bien preparatorias o ejecutivas, están orientadas a determinar qué o quién puede o no acceder a un recurso del sistema mediante una determinada acción. Con el cumplimiento de todas las medidas, se garantizará que nadie accederá a recursos sin la debida autorización. Adicionalmente, se establecerá la necesidad de que el uso del sistema quede registrado para detectar y reaccionar ante una incidencia de seguridad o fallo del sistema.

Toda medida de control de acceso busca el equilibrio entre la comodidad de uso y la protección del sistema, de tal forma que la seguridad se irá incrementando, en base a la categoría exigida. Así, en la categoría básica se primará la comodidad y en las categorías altas se primará la protección.

1.1.1.1. OP. ACC. 1. IDENTIFICACIÓN

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

La identificación de usuario se traduce en la necesidad de crear cuentas únicas e inequívocas para cada usuario y servicio, bien sea del dominio a través de cuentas de Directorio Activo o bien locales en los servidores, cuando se diera dicha necesidad. Dichas cuentas deberán ser gestionadas de tal forma que deban ser inhabilitadas cuando se den una serie de condicionantes:

a) El usuario deja la organización.

b) Cesa en la función para la cual se requería dicha cuenta.

c) La persona que lo autorizó emite una orden en contra.

Debe tenerse en consideración que nunca deberán existir dos cuentas iguales, de forma que éstas no puedan confundirse o bien imputarse acciones a usuarios diferentes.

La gestión de usuarios que aporta el Directorio Activo de Windows Server 2016 proporciona los mecanismos de seguridad suficientes para dar debido cumplimiento de esta medida. Adicionalmente, el operador deberá tener en consideración la funcionalidad de creación de cuentas, específicas para servicios, que le permitirán desvincularse de la gestión de dichas cuentas, reduciendo el TOC (tiempo de coste) de administración de las mismas y aumentando a la vez las garantías de seguridad. Así, la gestión de credenciales será mantenida por el propio Directorio Activo, siguiendo las políticas establecidas para la organización y realizando el cambio de las mismas, cuando debiera, en los servicios a los que se hubiera asignado. De esta forma, podrán mantenerse múltiples servicios, con cuentas específicas para ello, sin que el coste de administración repercuta en una gestión insegura. Toda la información de creación y gestión de cuentas de servicio en Windows Server 2016, así como las nuevas funcionalidades de las cuentas de servicio administradas de grupo la podrá localizar en la siguiente URL.

https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview

1.1.1.2. OP. ACC. 2. REQUISITOS DE ACCESO

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

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

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

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

Es necesario, en este sentido, que el operador conozca los requerimientos y procesos para la asignación de las listas de control de acceso (ACL), teniendo en consideración que es la base en las infraestructuras Microsoft para la concesión o no de acceso, así como qué estará permitido o denegado en cada circunstancia. Debe tener en consideración que Microsoft introduce la figura de los controles de acceso dinámicos, con condicionantes más avanzados para garantizar el acceso a la información, recursos y servicios. Las siguientes direcciones URL facilitan la información que proporciona el fabricante sobre los controles y vigilancia de acceso para Windows Server 2016, incluyendo los controles de acceso dinámicos.

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-8.1-and-8/jj134043(v=ws.11)

https://docs.microsoft.com/es-es/windows-server/identity/solution-guides/dynamic-access-control--scenario-overview

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

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

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

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

a) Desarrollo de operación.

b) Configuración y mantenimiento del sistema de operación.

c) Auditoría o supervisión de otra función.

Es factible realizar dichos procesos de segregación a través de los propios mecanismos que proporciona Windows Server 2016, así como las funcionalidades implicadas en la presente guía. Conforme a las necesidades planteadas en los dos primeros elementos, desarrollo de operaciones y la configuración, así como el mantenimiento del sistema de operación, el operador deberá tomar en consideración lo establecido en el Anexo A5 de la última revisión la guía CCN-STIC-570A. En dicho Anexo, además de otras cuestiones relativas a mejoras en la seguridad y procesos, se recogen los procedimientos que pueden ser llevados a cabo para la segregación de tareas, de tal forma que se pueden conceder determinados privilegios a usuarios concretos sin necesidad de facultarles de derechos completos. Así, se muestran ejemplos para delegar las tareas de agregar equipos al dominio a determinados usuarios, sin que estos tengan la necesidad de ser administradores del dominio o bien atribuirles los permisos para poder gestionar las cuentas del Directorio Activo con la misma premisa de no ser administradores.

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

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

Altamente vinculado al punto “1.1.1.2 OP. ACC. 2. REQUISITOS DE ACCESO”, este proceso requiere consolidación de los derechos de acceso, de tal forma que:

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

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

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

Como ya se comentó previamente, Windows Server 2016 se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso. La funcionalidad de delegación prevista en el Anexo A5 de la última revisión de la Guía CCN-STIC-570A facilitará la tarea de delegar tareas y controlar las autorizaciones asignadas.

Adicionalmente y siguiendo uno de los principios fundamentales de mínimo privilegio posible, a través de la aplicación de la presente guía se activarán las condiciones de control de cuenta de usuario. Aparecidas con Windows Vista y mejorada la experiencia de usuario y funcionalidad en sistemas posteriores, este componente debe entenderse como un mecanismo para impedir que el trabajo directo con usuarios con privilegios de administrador repercuta negativamente en la seguridad, al acometer todas las acciones con el máximo privilegio cuando éste no es siempre requerido.

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

El control de cuentas de usuarios (UAC) nace con la clara idea de hacer factible que un administrador sea consciente de cuándo una acción requiere un privilegio. Así, y en toda la sesión, el usuario "administrador" se convierte en un mero usuario estándar salvo cuando el sistema requiere de forma consciente la necesidad de la elevación.

Puesto que las condiciones de funcionalidad de UAC pueden establecerse desde la usabilidad hasta la máxima seguridad y atendiendo a los criterios marcados por el propio Esquema Nacional de Seguridad, las diferentes plantillas de seguridad que se generan para las diferentes categorías atenderán a estos criterios de criticidad. No obstante, y aunque se detallará más adelante, el operador puede conocer la funcionalidad del mecanismo de UAC a través de la información facilitada por el propio fabricante:

http://technet.microsoft.com/es-es/library/cc731416(v=ws.10).aspx

https://docs.microsoft.com/en-us/windows-server/security/user-account-control/how-user-account-control-works

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

1.1.1.5. OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN

Dentro de los procesos habituales en el manejo de los sistemas de la información, el relativo a la autenticación corresponde al primero a llevar a efecto. Antes de acceder a datos, gestionar recursos o tratar servicios es necesario indicar al sistema "quién eres".

El sistema de autenticación se puede traducir tecnológicamente mediante múltiples mecanismos, siendo el del empleo de una contraseña el más habitual pero no por ello el más

seguro, sino todo lo contrario. Los mecanismos de autenticación se deberán adecuar en función del nivel de criticidad de la información o el servicio atendiendo lógicamente a diferentes criterios.

Según establece el propio Esquema Nacional de Seguridad, a grandes rasgos estos criterios serán los siguientes:

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

b) Para la categoría media se desaconseja el empleo de password o claves concertadas, siendo recomendable el uso de sistemas físicos (Tokens), biométricos o certificados digitales.

c) Para la categoría alta, se prohíbe el uso de autenticadores basados en el empleo de claves concertadas. Se exige para ello el uso de dispositivos físicos o biometría. Para ello deberán emplearse algoritmos acreditados por el Centro Criptológico Nacional, recogidos en la guía CCN-STIC-808 de criptología de empleo en el ENS.

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

La presente guía tiene en consideración los siguientes aspectos para el desarrollo de plantillas de seguridad por categorías, enfocados en los procesos de autenticación:

a) Gestión y definición de política de contraseñas.

b) Gestión y definición de política para los bloqueos de cuenta.

c) Implementación de algoritmos para el almacenamiento de contraseñas cifradas.

d) Implementación de mecanismos para el bloqueo de cuentas de usuario y de servicio.

e) Permisividad para el empleo de mecanismos de algoritmos y criptografía basados en biometría, certificados o tarjetas inteligentes.

Debe tenerse en consideración que Windows Server 2016, así como el Directorio Activo, basan la implementación de los sistemas de autenticación en el empleo de contraseñas. No obstante, los proveedores de credenciales con los que cuenta Windows Server 2016 extienden los mecanismos de autenticación de Microsoft herederos de la antigua GINA (Graphic Identification and Authentication). Estos proveedores facultan la capacidad de introducir en los sistemas operativos mecanismos de autenticación que se adapten a cualquiera de las necesidades que pueden existir ahora y en el futuro.

Windows Server 2016 introduce además la capacidad de autenticación multifactor, como puede ser el empleo de un sistema de biometría y otro de tarjeta inteligente.

1.1.1.6. OP. ACC. 6. ACCESO LOCAL

Se considera acceso local aquel que se ha realizado desde los puestos de trabajo situados dentro de las propias instalaciones que tiene la organización. A efectos de esta guía, se tiene también en consideración la autenticación de tipo local que puede realizarse en los servidores Windows Server 2016.

El Esquema Nacional de Seguridad tiene en cuenta la aplicación de medidas diferentes atendiendo a la criticidad de servicios y sistemas. Así, en función de la categoría de seguridad, deberán aplicarse medidas:

a) En la categoría básica se prevendrán ataques para evitar intentos de ataques reiterados contra los sistemas de autenticación. Adicionalmente, la información proporcionada en caso de fallo en el acceso deberá ser mínima, siendo este hecho especialmente crítico en las aplicaciones web. También deberán registrarse los intentos satisfactorios y erróneos, así como informar a los usuarios de las obligaciones.

a) En la categoría media será una exigencia el proporcionar al usuario el detalle de la última vez que se ha autenticado.

b) En la categoría alta deberán existir limitaciones para la fecha y hora en las que se accede. También se facilitará, mediante identificación singular, la renovación de la autenticación, no bastando el hecho de hacerlo en la sesión iniciada.

Windows Server 2016, a través de la aplicación de políticas de grupo (GPO), permite establecer mecanismos para garantizar bloqueos de cuenta y proporcionar información al usuario, así como establecer medidas para garantizar un cambio seguro de las credenciales. Éstas serán aplicadas de forma progresiva en función de la categoría de seguridad exigido.

Para los sistemas de auditoría, como en el caso previo, se remite al operador a la guía CCN-STIC-859 de gestión y consolidación de registros de seguridad. Allí se detallan los procesos tanto para habilitar los registros de auditoría, que serán aplicados por políticas de seguridad, así como los procesos para recogerlos e interpretarlos.

1.1.1.7. OP. ACC. 7. ACCESO REMOTO

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

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

Windows Server 2016 faculta el empleo de protocolos seguros para las comunicaciones y los procesos de autenticación. Sin embargo, no todos los protocolos empleados históricamente por los productos de Microsoft se pueden considerar, a día de hoy, seguros. La presente guía tiene en consideración este detalle y, por lo tanto, habilitará o deshabilitará, en su defecto, aquellos protocolos que son considerados, o no, seguros. Esto incluye los correspondientes a autenticaciones empleadas en redes locales o remotas.

1.1.2. EXPLOTACIÓN

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

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

1.1.2.1. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD

Los equipos, antes de su entrada en producción, deberán configurarse de tal forma que:

a) Se retiren cuentas y contraseñas estándar.

b) Se aplique la regla de mínima funcionalidad.

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

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

Adicionalmente se deshabilitarán, como parte de los mecanismos de mínima funcionalidad y mínima exposición de la información manejada, todos aquellos procesos que pudieran implicar el envío de información al fabricante o todos aquellos servicios automatizados susceptibles de reportar datos o funcionalidad de los servidores.

1.1.2.2. OP. EXP. 4. MANTENIMIENTO

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

En este sentido, la presente guía sigue los patrones establecidos por Microsoft como fabricante de Windows Server 2016. Debe tenerse en consideración que este Sistema Operativo es un elemento en constante evolución que, ante la aparición de un riesgo de seguridad, deberá dotar de los mecanismos necesarios para paliar el problema. Para ello, Microsoft hace una constante difusión de actualizaciones de seguridad que se deberán evaluar e implementar sobre los servidores, con objeto de mantener las garantías de seguridad necesarias.

No es objeto de esta guía especificar los mecanismos a emplear para mantener actualizados los sistemas. Las plantillas de seguridad basarán las condiciones para que los sistemas puedan ser actualizados, empleando para ello el servicio de actualizaciones de Microsoft existente en Windows Server 2016. Podrá encontrar más información relativa a la gestión e implementación de sistemas de actualizaciones en la siguiente dirección URL:

http://support.microsoft.com/kb/919772/es

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

Aplicables en las categorías altas de seguridad, se deberán implementar mecanismos para garantizar la trazabilidad de las acciones de los usuarios. Para ello, se deberá conocer:

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

b) La actividad de los usuarios y especialmente la de los operadores y administradores del sistema en el momento en que pueden acceder a la configuración y actuar en el mantenimiento del mismo.

c) Las actividades realizadas con éxito, así como los intentos infructuosos.

La determinación de las actividades y el nivel de detalle se determinarán en base al análisis de riesgos que se haya realizado sobre el sistema.

Windows Server 2016 implementa mecanismos para la auditoría de los sistemas e infraestructuras. El problema consiste en que, de forma predeterminada, los datos son almacenados localmente. Existen, no obstante, mecanismos nativos para la suscripción y recolección de eventos. Tal y como ya se ha comentado previamente, la guía CCN-STIC-859 permitirá establecer los procedimientos para la recogida y análisis de los registros de auditoria, desde múltiples sistemas, permitiendo establecer mecanismos de correlación.

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

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

a) Determinar el período de retención de los registros.

b) Asegurar fecha y hora.

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

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

Nuevamente, en la guía CCN-STIC-859, se articulan los mecanismos para garantizar la disponibilidad y retención de los registros, así como los procedimientos operativos para su salvaguarda.

1.2. MEDIDAS DE PROTECCIÓN

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

Solo éstas últimas se tendrán en consideración para su implementación en la presente guía y de ellas solo un número limitado es de aplicación sobre las funcionalidades del propio sistema operativo servidor. La mayor parte de ellas son de aplicación en la red o cuando un sistema tipo portátil sale de la organización, cuestión que no se considera de aplicación a un servidor que se considera ubicado en un entorno estable dentro del centro de procesamiento de datos (CPD) que tuviera la organización.

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

1.2.1. PROTECCIÓN DE LOS EQUIPOS

Las medidas de protección de los equipos cubren todos aquellos mecanismos que son necesarios para garantizar una configuración de seguridad válida para el sistema, así como para mantener la propia privacidad del trabajo desarrollado.

Dentro de las medidas, se articulan la aplicación de mecanismos de índole tecnológica y otras de tipo física. Entre estas últimas, pueden localizarse las correspondientes a un puesto de trabajo despejado.

Aunque esta guía de seguridad se encuentra orientada a un sistema operativo de servidor, se tienen en consideración aquellas medidas que, siendo establecidas para un puesto de trabajo, le es de completa aplicación, por ejemplo, la necesidad de realizar un bloqueo del puesto de trabajo.

1.2.1.1. MP. EQ. 2. BLOQUEO DE PUESTO DE TRABAJO

Aplicable desde la categoría media, se establece la necesidad de realizar un bloqueo de la cuenta toda vez que se haya producido una inactividad en el sistema tras un periodo de tiempo prudencial. Dicho periodo de tiempo deberá ser establecido por política de seguridad.

Adicionalmente a todos aquellos sistemas de categoría alta, deberán cancelarse las sesiones abiertas cuando se supere un periodo de tiempo de actividad superior al anteriormente planteado. Estos controles serán aplicables en Windows Server 2016 mediante la aplicación de objetos de política de grupo en el dominio.

1.2.2. PROTECCIÓN DE LAS COMUNICACIONES

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

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

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

Se deberá asegurar la autenticidad del otro extremo en un canal de comunicaciones antes de proceder al intercambio de datos entre los mismos. Además, deberán prevenirse ataques activos, garantizando que los mismos serán al menos detectados, permitiendo activarse los procedimientos que se hubieran previsto en el tratamiento frente a incidentes.

En aquellos sistemas en que sea de aplicación la categoría media, además de los mecanismos anteriores aplicables a la categoría básica, les será de aplicación la necesidad de implementar redes virtuales privadas cuando su comunicación se realice a través de redes fuera de la organización o del propio dominio de la seguridad. Para ello, se deberán tener en consideración los algoritmos que han sido acreditados por el Centro Criptológico Nacional.

Para aquellos entornos con sistemas o información catalogados como de categoría alta, es recomendable el empleo de dispositivos de hardware para el establecimiento y utilización de redes virtuales privadas, frente a soluciones de tipo software. Se deberán tener en consideración los productos que se encuentran certificados y acreditados.

A través de controles centralizados en plantillas de seguridad, se establecerán mecanismos que controlen el acceso a los servidores Windows Server 2016 mediante el empleo del firewall en su modalidad avanzada. Aunque se tratará en extensión en un anexo de la presente guía, el operador podrá conocer todos los detalles de esta solución a través de la información que proporciona el fabricante:

https://docs.microsoft.com/en-us/windows/security/identity-protection/windows-firewall/windows-firewall-with-advanced-security

Además, se establecerán, por políticas de grupo, los controles relativos a la protección de la autenticación, habilitando solo aquellos protocolos que son válidos y seguros.

2. RESUMEN Y APLICACIÓN DE MEDIDAS EN WINDOWS SERVER 2016

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

Control	Medida	Mecanismo de aplicación
OP. ACC. 1	Segregación de roles y tareas	Revisión e implementación de mecanismos articulados en el Anexo A5de la guía CCN-STIC-570A, adaptándolos a la organización.
OP. ACC. 1	Auditoría y supervisión de actividad	Revisión e implementación de guía CCN-STIC-859, adaptándolos a la organización.
OP. ACC. 4	Gestión de derechos de acceso	Revisión e implementación de mecanismos articulados en el Anexo A5 de la guía CCN-STIC-570A, adaptándolos a la organización.
OP. ACC. 4	Control de cuentas de usuario	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. ACC. 5	Política de contraseñas	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. ACC. 5	Protocolos de autenticación local	Implementación de GPO a través de plantillas facilitadas en la presente guía.

Control	Medida	Mecanismo de aplicación
OP. ACC. 6	Bloqueo de cuentas	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. ACC. 7	Protocolos de autenticación en red	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. EXP. 2	Control de funcionalidad de servicios para garantizar el principio de mínima funcionalidad	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. EXP. 2	Protección de aplicaciones de sistema para garantizar el principio de mínima funcionalidad.	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. EXP. 4	Mantenimiento del Sistema Operativo	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. EXP. 8	Registro de actividad de los usuarios	Revisión e implementación de guía CCN-STIC-859, adaptándolos a la organización.
OP. EXP. 10	Protección de los registros de actividad	Revisión e implementación de guía CCN-STIC-859, adaptándolos a la organización.
MP. EQ. 2	Bloqueo de los puestos de trabajo	Implementación de GPO a través de plantillas facilitadas en la presente guía.
MP. COM. 3	Protección del sistema mediante implementación de firewall.	Implementación de GPO a través de plantillas facilitadas en la presente guía. Implementación de configuración de firewall avanzado a nivel local según el ANEXO A.5.1 en la presente guía.
MP. COM. 3	Protección de la autenticación.	Implementación de GPO a través de plantillas facilitadas en la presente guía.

ANEXO A.2. CATEGORÍA BÁSICA

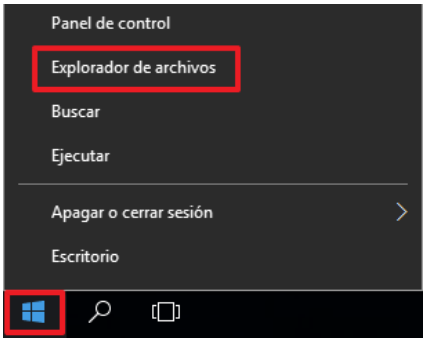
ANEXO A.2.1. GUÍA PASO A PASO CONTROLADOR DE DOMINIO QUE LE SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

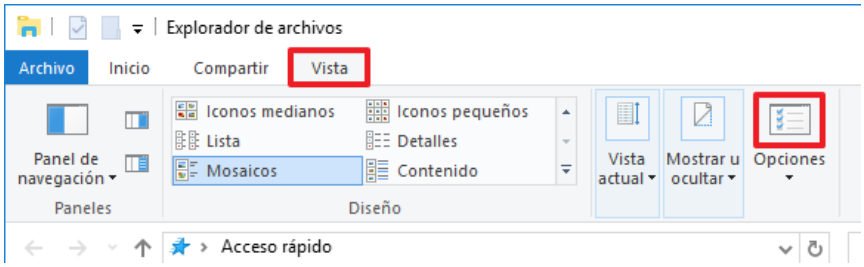
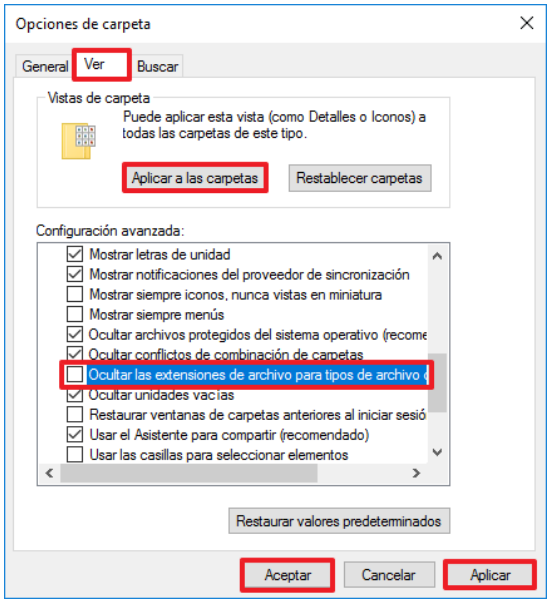
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se emplee Windows Server 2016 con una categorización de seguridad baja según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar la categoría 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 la categoría básica, deberá realizar las implementaciones según se referencian en el presente anexo.

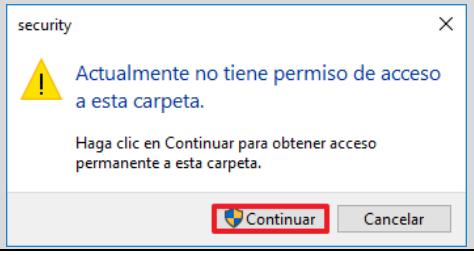
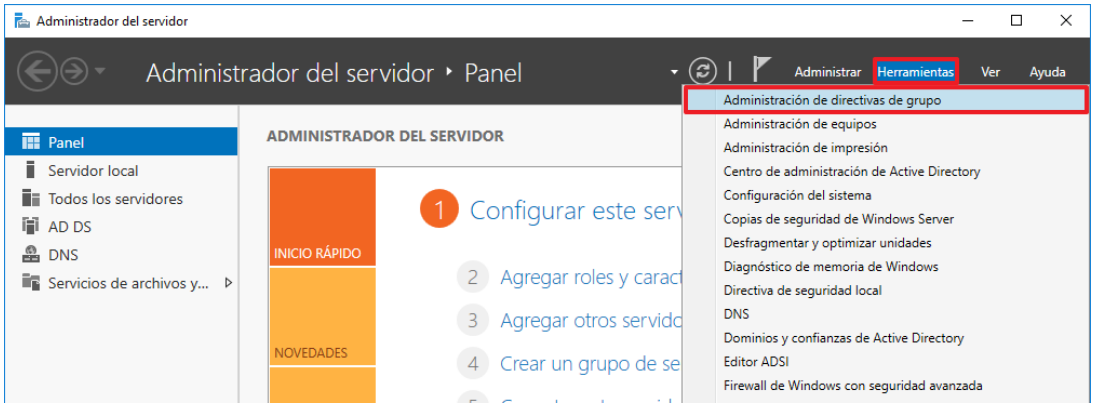
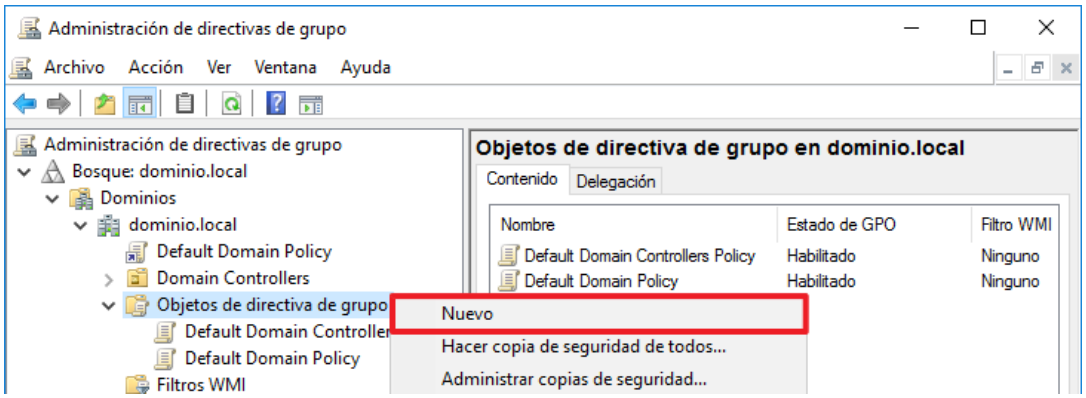
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

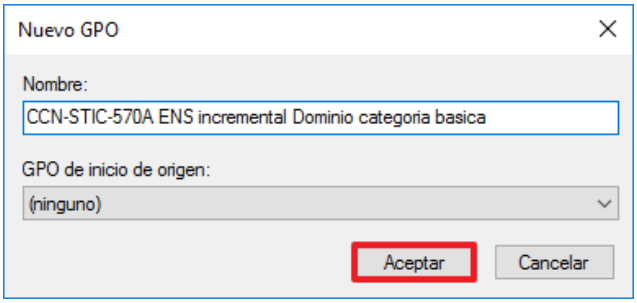
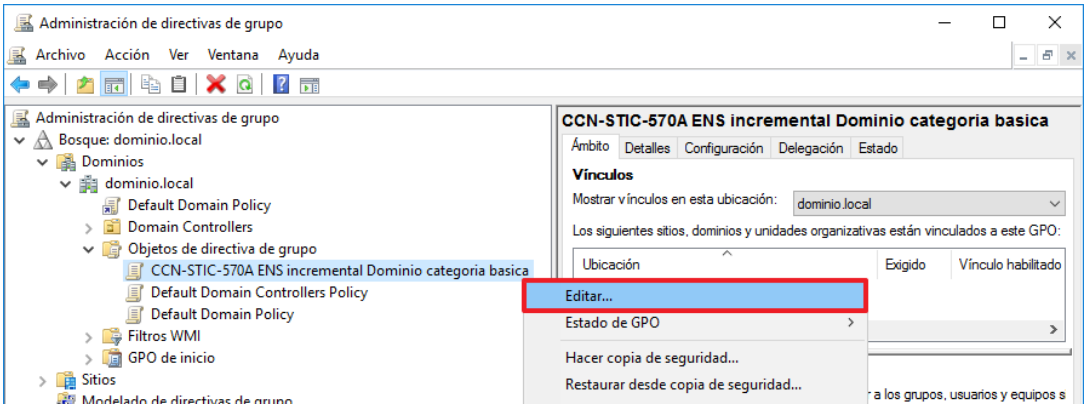
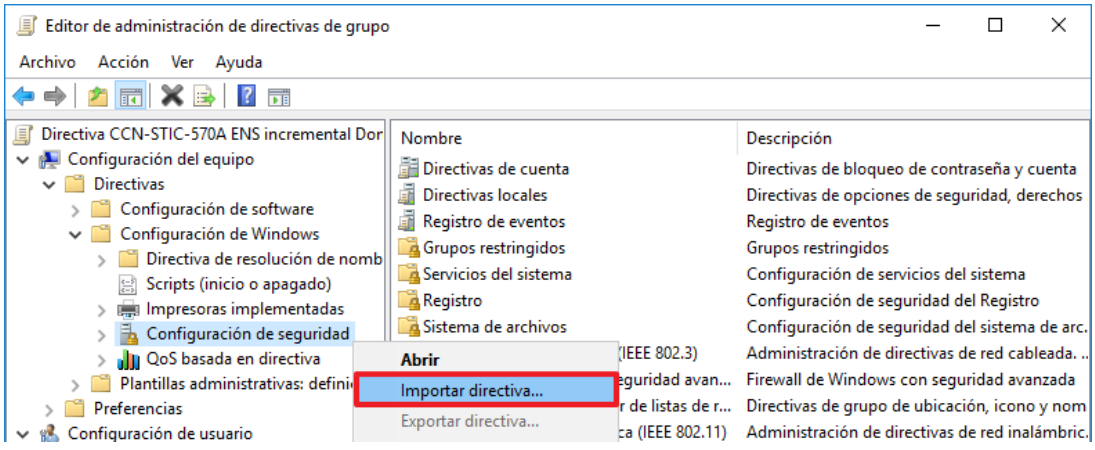
1. PREPARACIÓN DE DOMINIO

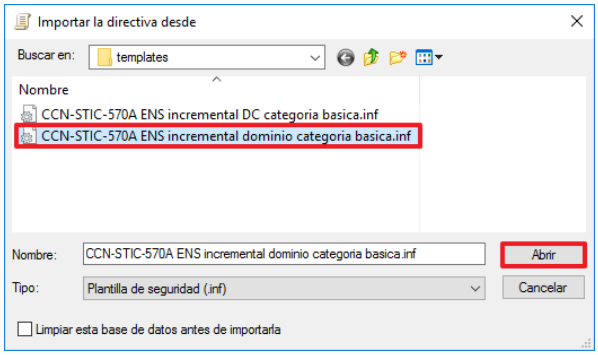
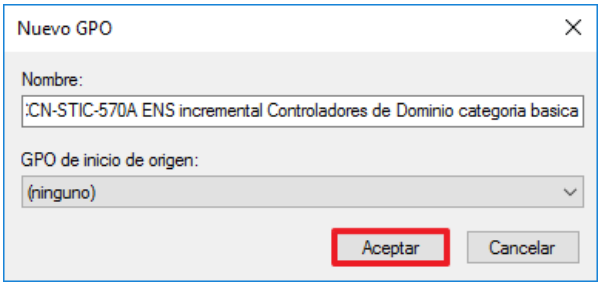
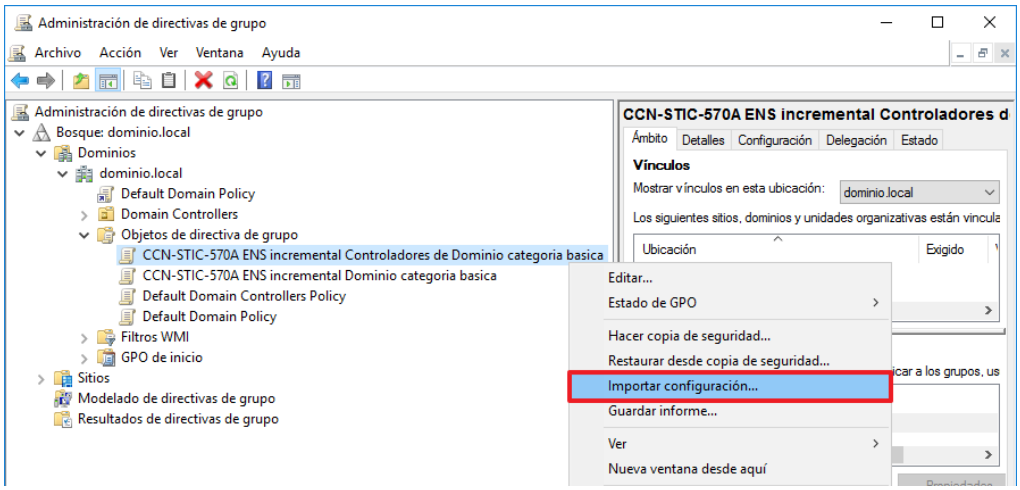
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se realizará la implementación de las plantillas de seguridad. Solo es necesario realizar este procedimiento una vez.

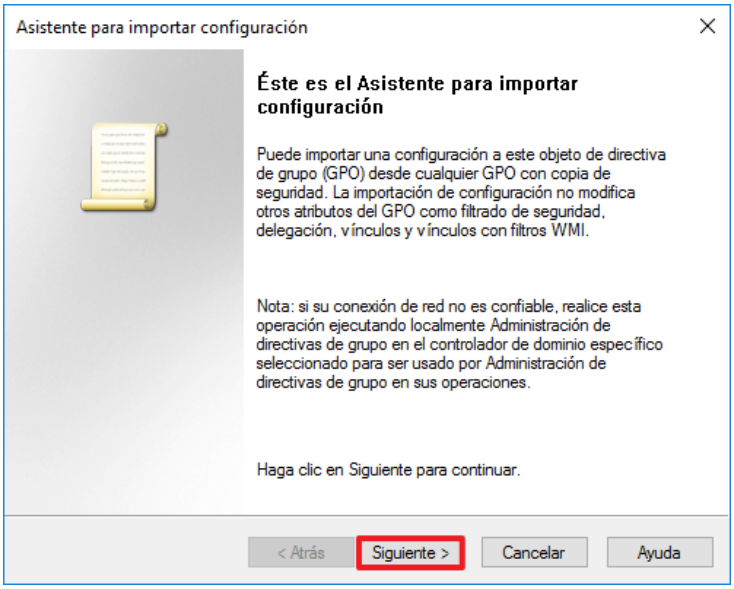
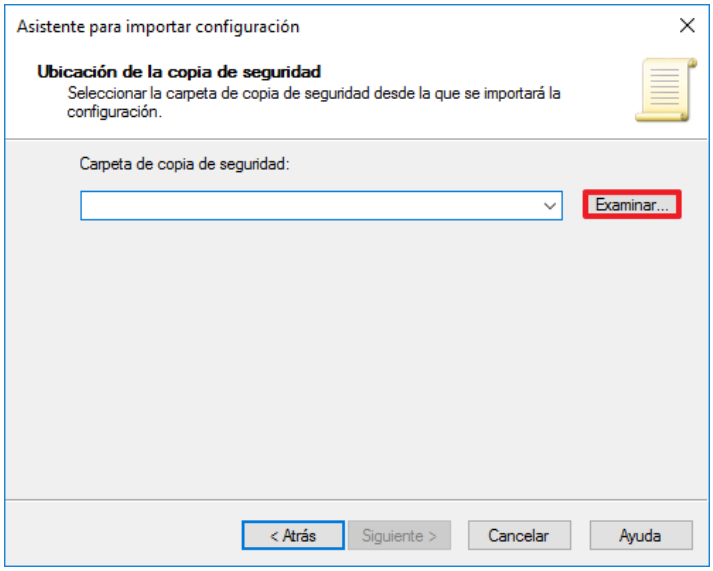
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Cree el directorio “Scripts” en la unidad C:\.
4.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts". **Nota**: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-570A”.
5.	Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de “Inicio” con el botón derecho y seleccione “Explorador de archivos”. 

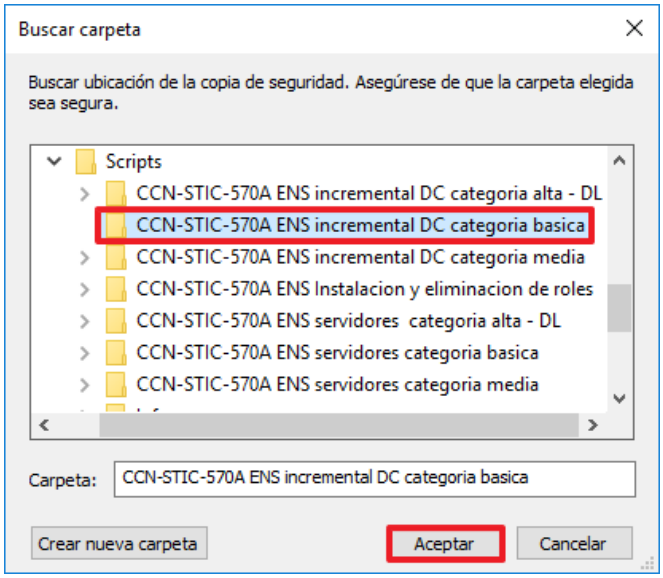
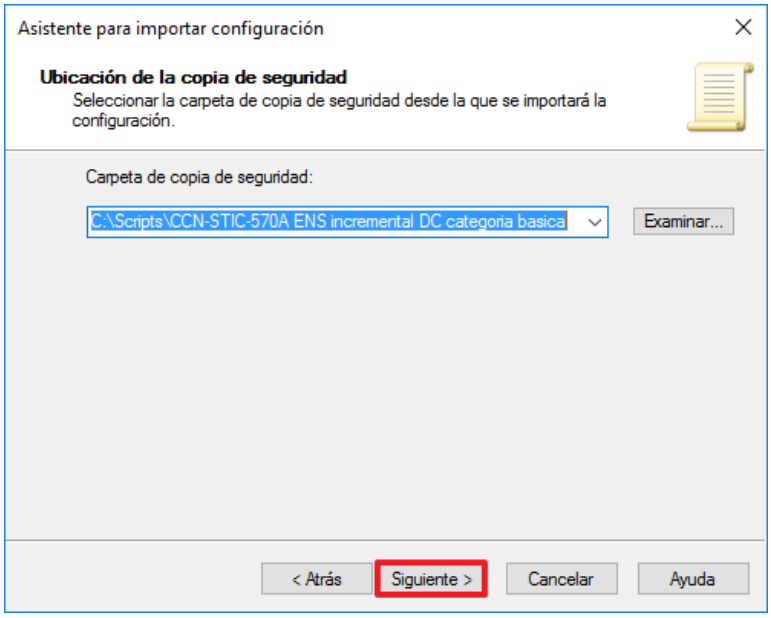
Paso	Descripción
6.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”. 
7.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 
8.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio: – CCN-STIC-570A ENS incremental DC categoria basica (directorio) – CCN-STIC-570A ENS servidores categoria basica (directorio) – CCN-STIC-570A ENS incremental DC categoria basica.inf – CCN-STIC-570A ENS incremental dominio categoria basica.inf – CCN-STIC-570A ENS Incremental servidores categoria basica.inf

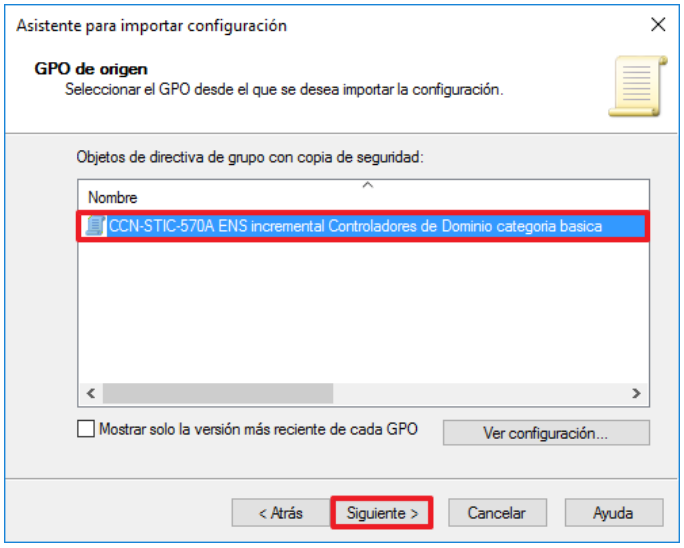
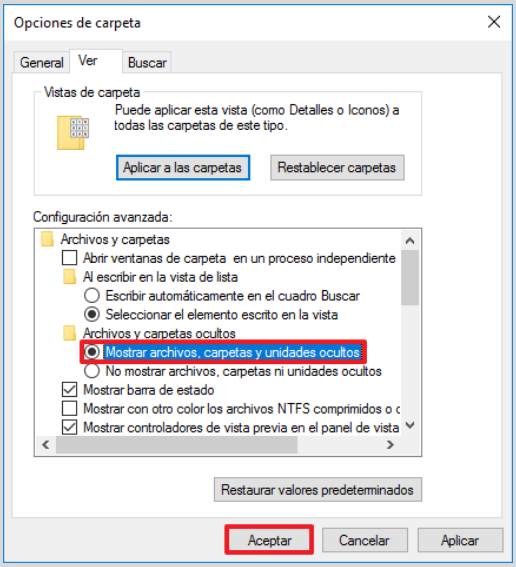
Paso	Descripción
9.	Copie los ficheros “CCN-STIC-570A ENS incremental dominio categoría basica.inf” y “CCN-STIC-570A ENS incremental DC categoria basica.inf, al directorio “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota**: Según la configuración de seguridad de UAC, el sistema podría solicitar la elevación de privilegios, en este caso, pulse “Continuar”. 
10.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”** 
11.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”.
12.	Pulse con el botón derecho, sobre dicha y carpeta y seleccione la opción “Nuevo”. 

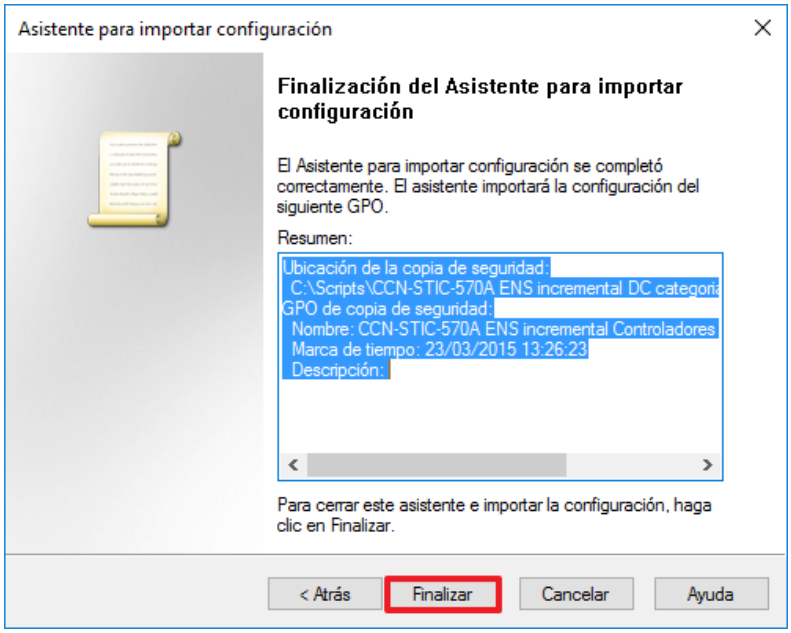
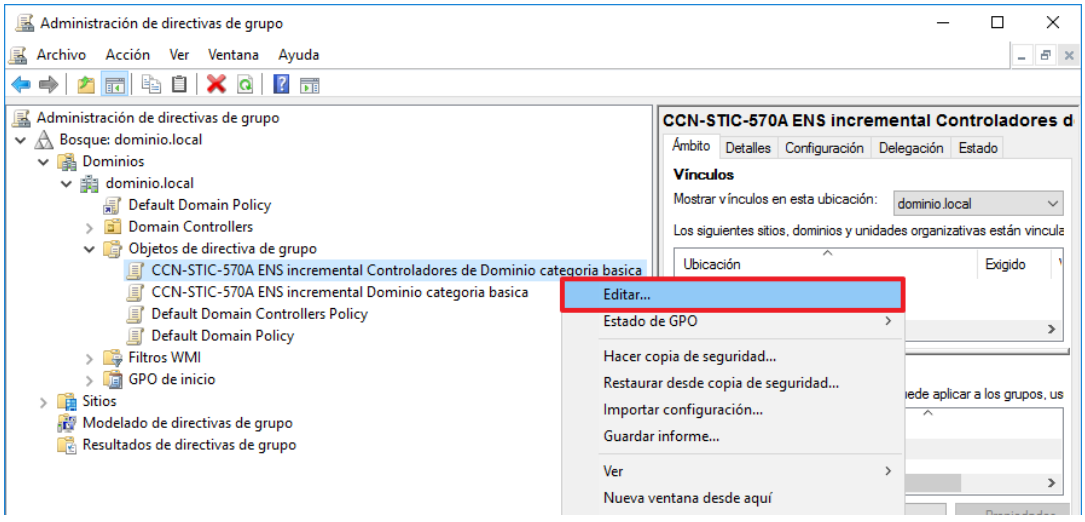
Paso	Descripción
13.	Introduzca como nombre “CCN-STIC-570A ENS incremental Dominio categoria basica” y pulse el botón “Aceptar”. 
14.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
15.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**
16.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva…”. 

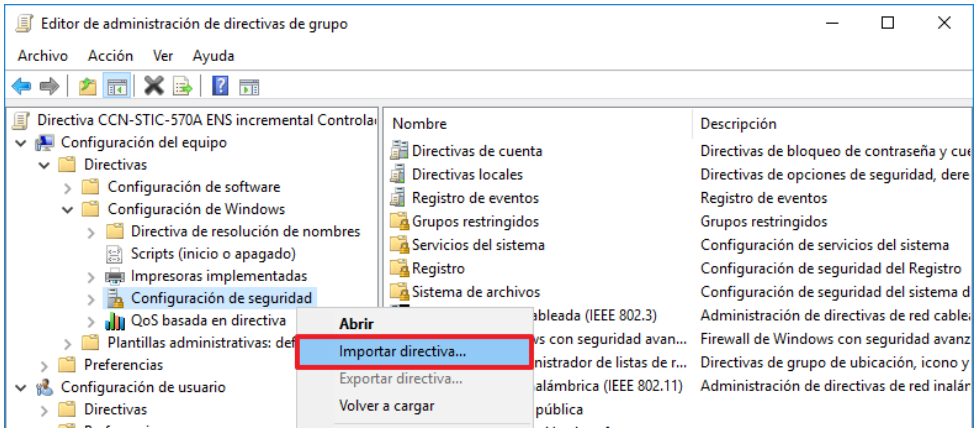
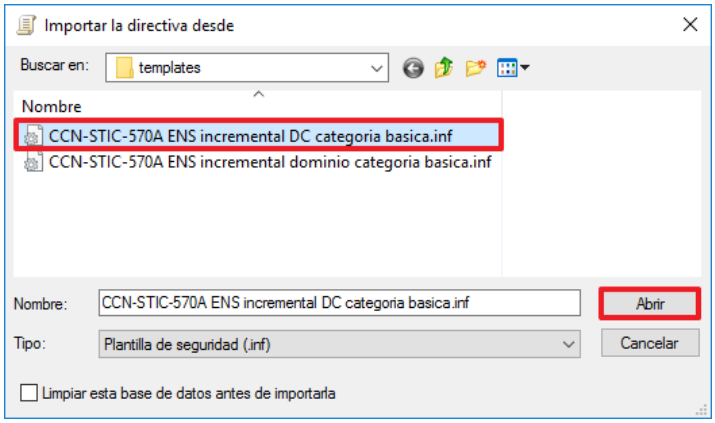
Paso	Descripción
17.	Seleccione de la ruta “C:\Windows\Security\Templates” el fichero “CCN-STIC-570A ENS incremental Dominio categoria basica” y pulse el botón “Abrir”. 
18.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
19.	Vuelva a pulsar con el botón derecho sobre el contenedor de objetos de directiva de grupo y seleccione la opción “Nuevo”.
20.	Introduzca como nombre “CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica” y pulse el botón “Aceptar”. 
21.	La nueva política requiere una configuración de plantillas administrativas. Para ello y seleccionando la política, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración…”. 

Paso	Descripción
22.	En el asistente de importación de configuración, pulse el botón “Siguiente >”. 
23.	En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.
24.	En “Carpeta de copia de seguridad”, pulse el botón “Examinar...”. 

Paso	Descripción
25.	Seleccione la carpeta “CCN-STIC-570A ENS incremental DC categoria basica” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 
26.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada. 

Paso	Descripción
27.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-570A incremental DC categoria basica” y pulse el botón “Siguiente >”.  **Nota:** Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero “manifest.xml”. Este es un fichero oculto y, por lo tanto, debe mostrar en “opciones de carpeta” la opción “Mostrar archivos, carpetas y unidades ocultos”. 
28.	En la pantalla de examen, pulse el botón “Siguiente >”.

Paso	Descripción
29.	Para completar el asistente pulse el botón “Finalizar”. 
30.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración.
31.	A continuación, seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
32.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**

Paso	Descripción
33.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva…”. 
34.	Seleccione de la ruta “C:\Windows\Security\Templates” el fichero “CCN-STIC-570A ENS incremental DC categoria basica” y pulse el botón “Abrir”. 
35.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
36.	Las políticas se encuentran ya creadas correctamente. No obstante, no se aplicarán hasta más adelante, una vez que haya tenido en cuenta y aplicado todas las consideraciones adicionales que se mostrarán en el siguiente punto del presente anexo. Cierre la herramienta “Administración de Directivas de Grupo”.

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

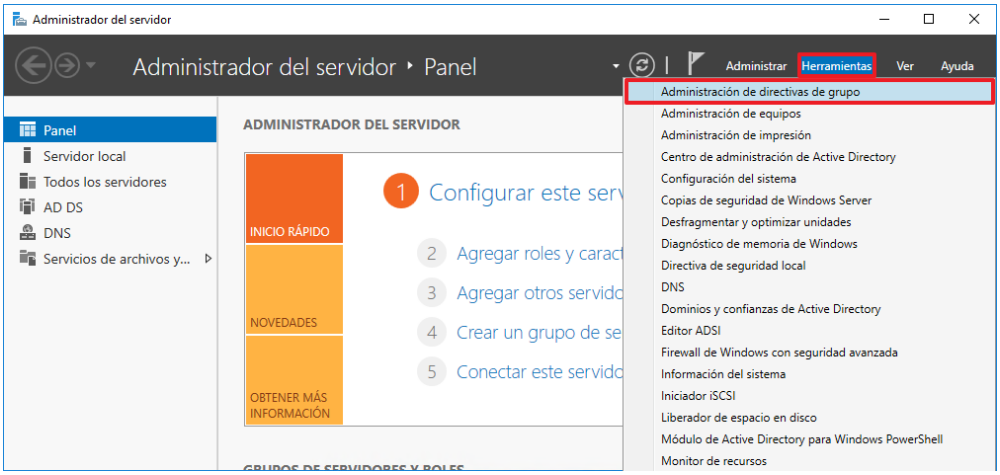
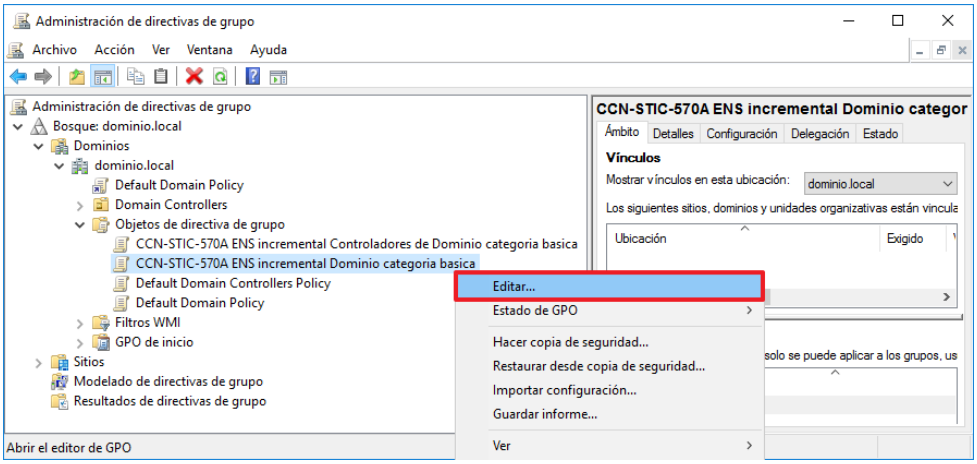
El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración. Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría

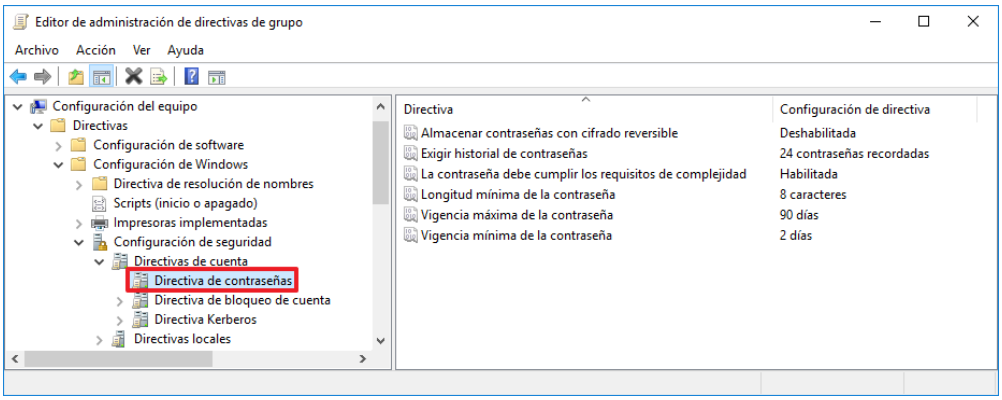
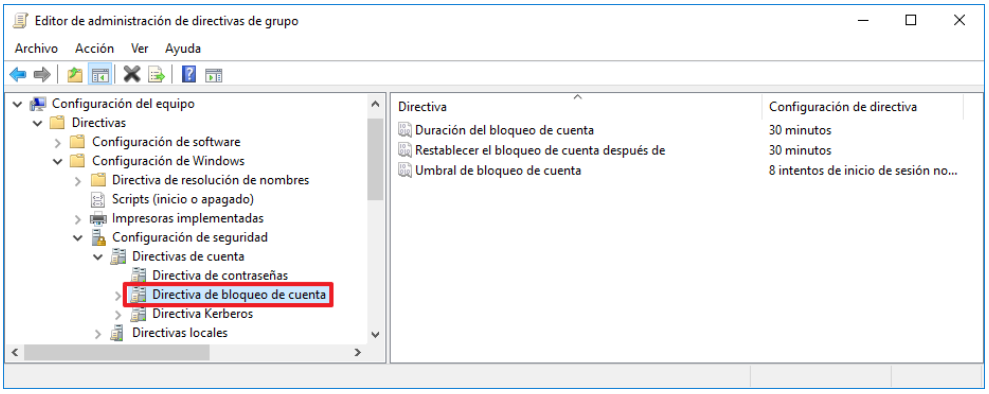
básica. No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

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

2.1. CONTRASEÑAS Y BLOQUEO DE CUENTAS

Es factible que su organización cuente con una política de contraseña consolidada. La implementación de la política que se aplicará sobre el dominio "CCN-STIC-570A ENS incremental Dominio categoria basica" aplicará una de forma particular. Deberá evaluarla para determinar si esta configuración le es válida o por el contrario debe adaptarla a las condiciones de su organización.

Paso	Descripción
37.	Para evaluar y realizar la modificación oportuna inicie la herramienta "Administración de Directivas de Grupo". Para ello y sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"** 
38.	Edite el objeto de GPO "CCN-STIC-570A ENS incremental Dominio categoria basica". Para ello seleccione dicha política y seleccione la opción "Editar…". 

Paso	Descripción
39.	Despliegue la política y sitúese en la siguiente ruta: **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseñas"** 
40.	Evalúe la política de contraseñas y modifíquela convenientemente. **Nota:** Debe tener en consideración que si su política de credenciales es menos rigurosa que la marcada en la configuración deseada, se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de contraseñas a lo marcado por la configuración recomendada.
41.	De forma similar a lo anterior, deberá evaluar la política de bloqueo de cuenta. Para ello y sin cerrar la política, seleccione la "Directiva de bloqueo de cuenta" que encontrará al mismo nivel que la directiva de contraseñas. 
42.	Evalúe la política de bloqueo de cuenta y modifíquela convenientemente. **Nota:** Debe tener en consideración que, si su política de bloqueo de cuenta es menos rigurosa que la marcada en la configuración deseada, se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de bloqueo de cuenta a lo marcado por la configuración recomendada.
43.	Cierre el "Editor de administración de directivas de grupo".
44.	Cierre la herramienta "Administración de directivas de grupo".

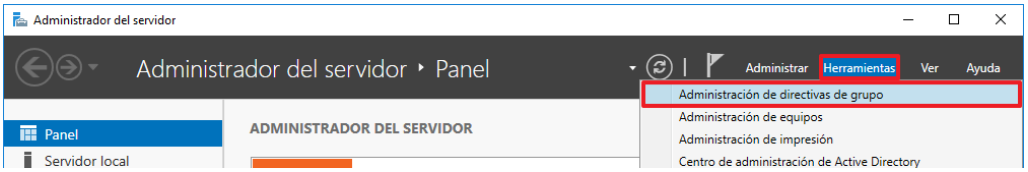
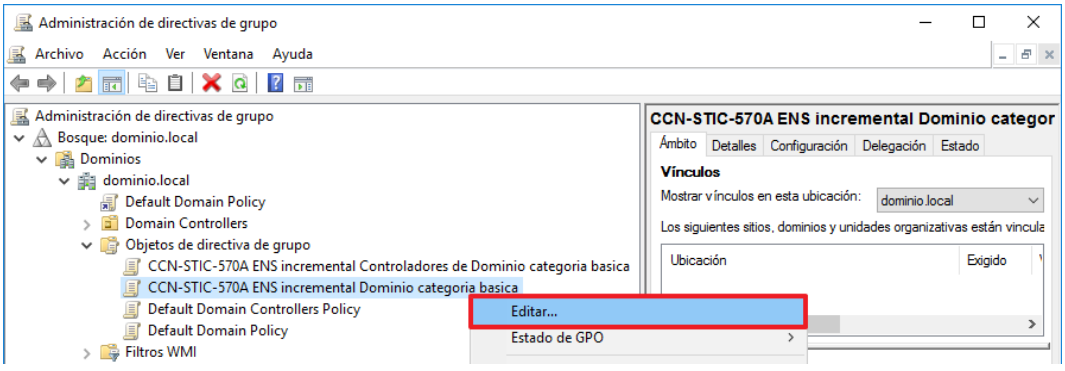
2.2. INFORMACIÓN DE OBLIGACIONES

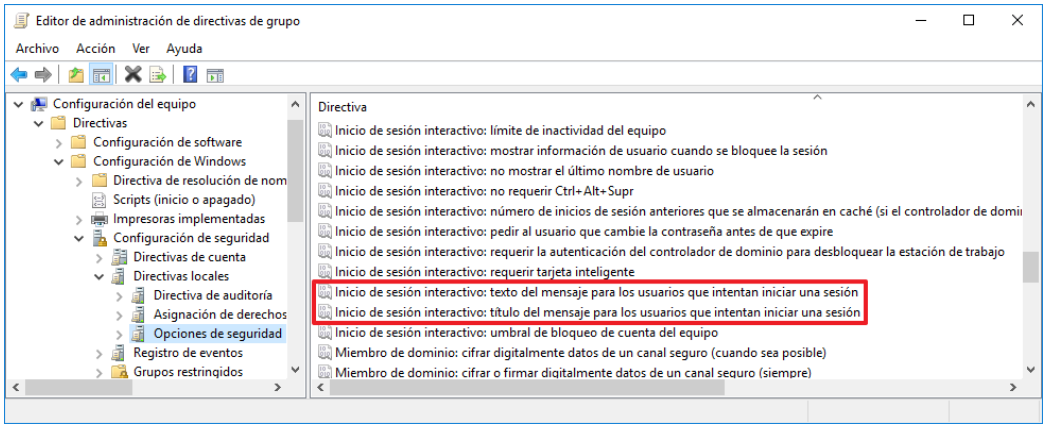
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional para el acceso local, consiste en la necesidad de informar al usuario de sus obligaciones.

Los sistemas Windows presentan mecanismos para implementar mensajes que son advertidos al usuario cuando va a realizar el inicio de la sesión. Aunque pudieran emplearse otros tales como la ejecución de scripts, el empleo de este mecanismo es altamente recomendable. Debe, no obstante, tomarse en consideración que su organización ya está empleando este mecanismo para notificar otros detalles como los marcados por el Reglamento Europeo General de Protección de Datos (GDPR) 2016/679/CE y la Ley Orgánica 15/1999 de protección de datos de carácter personal.

Si fuera así, modifique el mensaje mostrado para adaptarlo también al cumplimiento del ENS según lo estipulado en la política de seguridad de su organización.

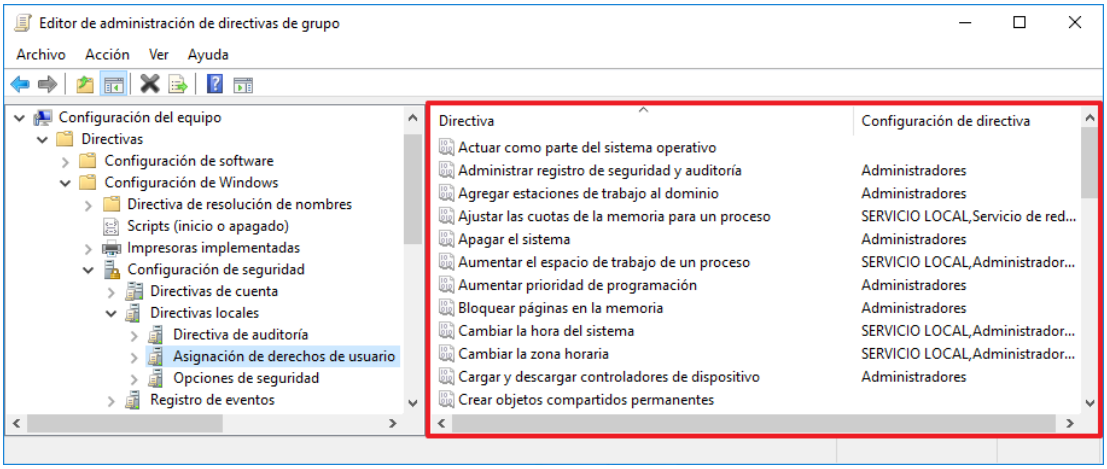
Si su organización no está haciendo uso de este mecanismo, siga los siguientes pasos para habilitar el sistema de advertencia, con objeto de informar al usuario de sus obligaciones, según quede estipulado en la política de seguridad de la organización.

Paso	Descripción
45.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”** 
46.	Edite el objeto de GPO “CCN-STIC-570A ENS incremental Dominio categoria basica”. Para ello seleccione dicha política y seleccione la opción “Editar…”. 
47.	Despliegue la política y sitúese en la siguiente ruta: **“Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**.

Paso	Descripción
48.	Identifique las directivas “Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión” e “Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión”. 
49.	Edite ambas directivas incluyendo el título de la advertencia y el mensaje a facilitar a los usuarios según se estipule en las políticas de seguridad de la organización.
50.	Cierre la política de seguridad.
51.	Cierre “Administración de Directivas de Grupo”.

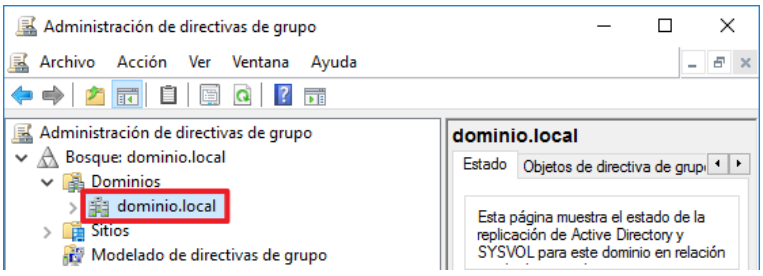
2.3. ASIGNACIÓN DE DERECHOS DE USUARIO

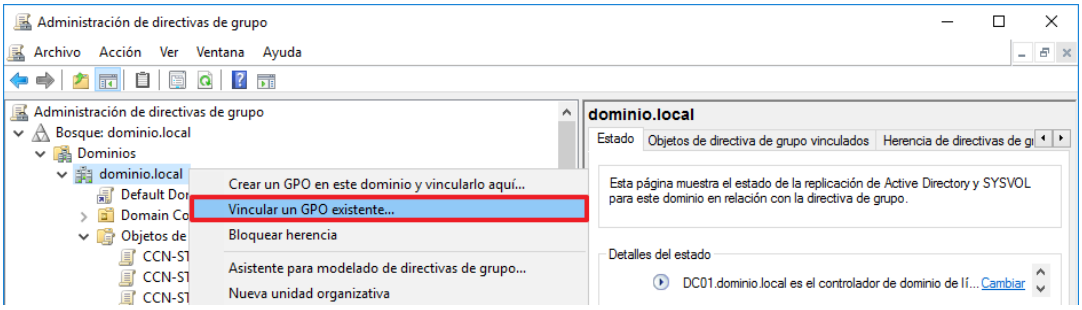
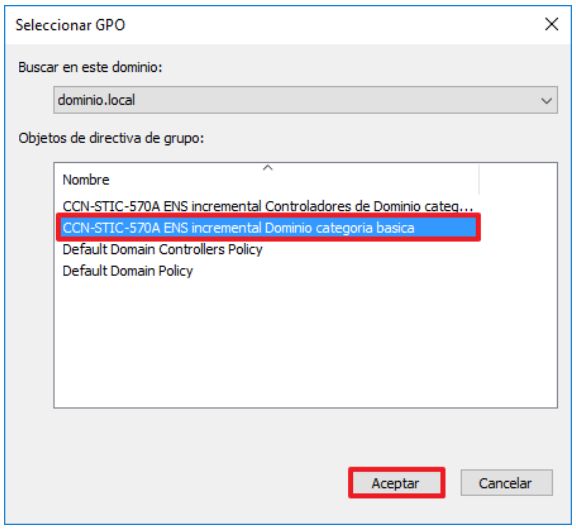
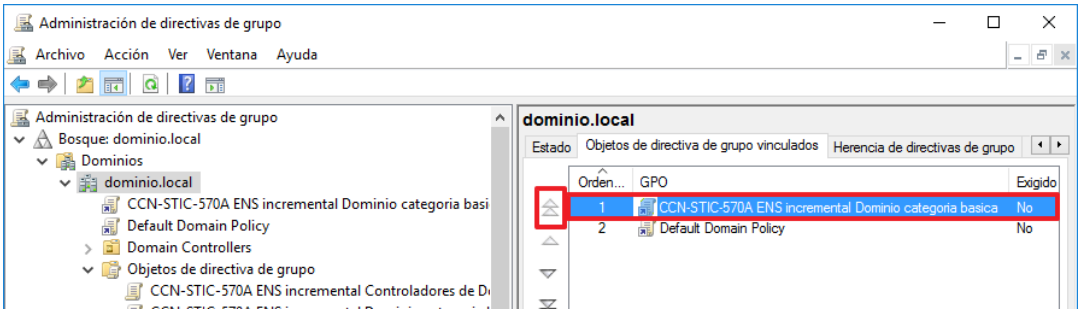
Paso	Descripción
52.	Los objetos de políticas de grupo para Controladores de Dominio y Servidores miembros especifican unos derechos de usuario siguiendo planteamientos de seguridad que aplican los principios de mínimo privilegio y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les hayan asignado derechos determinados para la administración o gestión de los sistemas. Si esto fuera así, deberá realizar las modificaciones pertinentes sobre el objeto de política de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica”.
53.	Edite la política de grupo correspondiente iniciando la herramienta “Administración de Directivas de Grupo” y seleccionando la política a modificar. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”** Sobre el objeto de GPO que se quiere modificar, deberá pulsar clic derecho y seleccionar “Editar” en el menú desplegado.

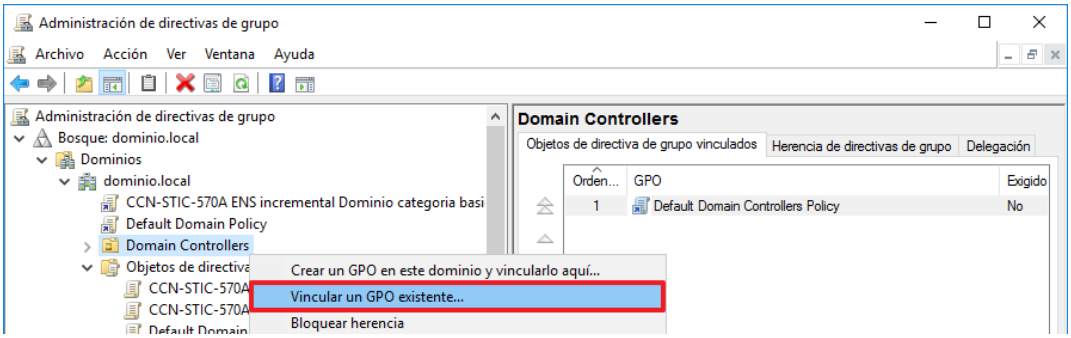
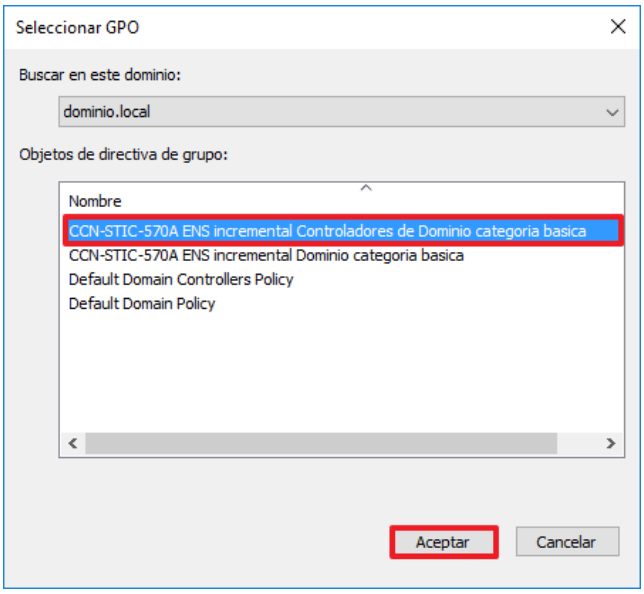
Paso	Descripción
54.	Una vez abierto el "Editor de administración de directivas de grupo", despliegue la política y sitúese en la siguiente ruta: **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"** 
55.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
56.	Guarde la configuración cerrando la ventana de editor de administración de directivas de grupo.

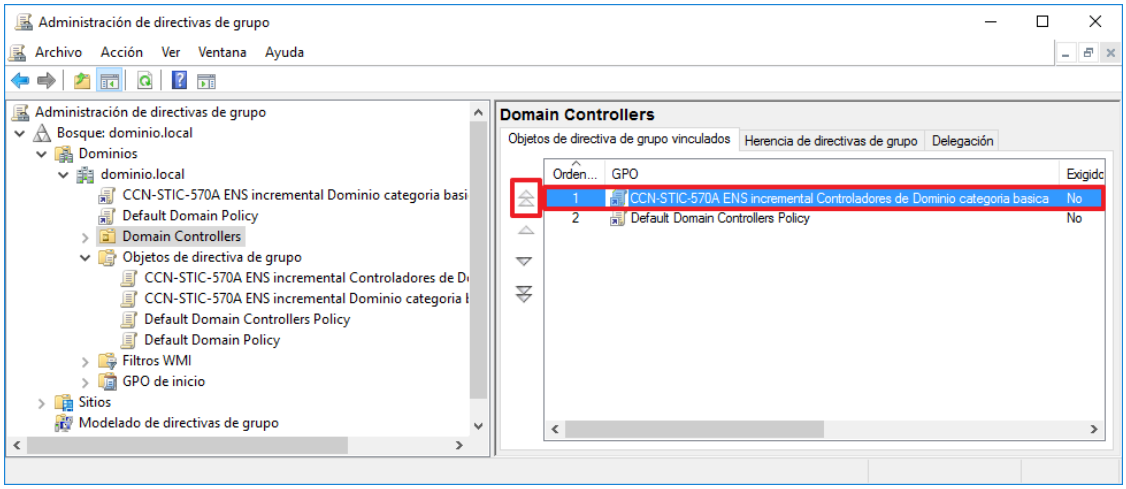
3. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

El presente punto establece la aplicación de las políticas de seguridad, toda vez que se han tenido en consideración las condiciones definidas en el punto previo.

Paso	Descripción
57.	Inicie la herramienta de administración de directivas de grupo.
58.	Despliegue el bloque y posiciónese sobre su dominio.  **Nota:** En el ejemplo el dominio utilizado se denomina "dominio.local".

Paso	Descripción
59.	Pulse con el botón derecho sobre el mismo y seleccione la opción “Vincular un GPO existente…”. 
60.	Seleccione la política “CCN-STIC-570A ENS incremental Dominio categoria basica” y pulse el botón “Aceptar”. 
61.	Una vez agregado, en el panel derecho seleccione la pestaña “Objetos de directiva de grupo vinculados” y seleccione la política “CCN-STIC 570A ENS incremental Dominio categoria basica”.
62.	Pulse el botón con la flecha que apunta hacia arriba hasta situar la política “CCN-STIC 570A ENS incremental Dominio categoria basica” en primer lugar dentro del orden de vínculo. 

Paso	Descripción
63.	Seleccione la Unidad Organizativa “Domain Controllers” y seleccione la opción “Vincular un GPO existente…”.  **Nota:** Si sus controladores de dominio se encontraran en otra ubicación vincule la siguiente GPO en dicha OU.
64.	Seleccione la política “CCN-STIC-570A ENS incremental Controladores de dominio” y pulse el botón “Aceptar”. 

Paso	Descripción
65.	Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica” y pulse el botón con la flecha que apunta hacia arriba hasta situarla en primer lugar dentro del orden de vínculo. 
66.	Cierre la herramienta de administración de directivas de grupo.
67.	Elimine la carpeta “C:\Scripts”.

4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD EN LOS EQUIPOS

Las configuraciones planteadas a través de la presente guía han sido ampliamente probadas en entornos de operativa Microsoft. No obstante, no se han podido probar todas las condiciones existentes, ni con las peculiaridades de cada organización. Bajo determinadas condiciones, pudieran suceder algunas incidencias que se describen a continuación, así como su resolución.

Debe tenerse en consideración que la resolución consiste en rebajar algunos de los mecanismos de seguridad descritos en la presente guía. Por lo tanto, deberá plantearse una solución que, de forma paulatina, permita alcanzar el estado de seguridad deseado y recomendado por la presente guía.

4.1. CIFRADOS PERMITIDOS PARA KERBEROS

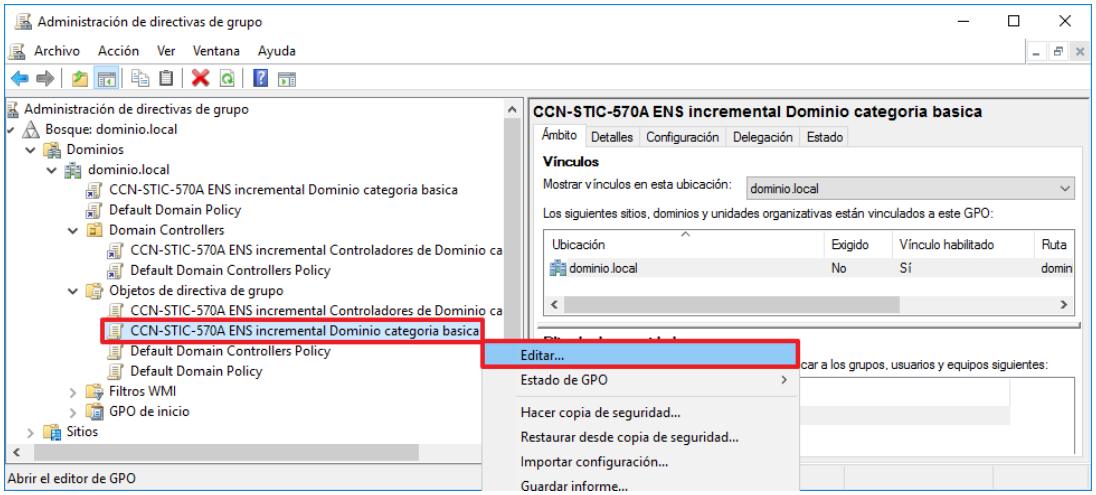
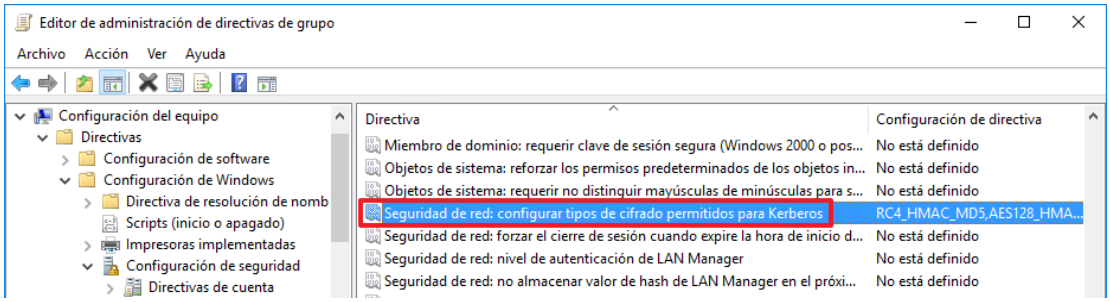
Un elemento significativo para los procesos de autenticación, en el marco de un dominio, lo corresponde la autenticación Kerberos. El proceso de validación se realiza mediante sistemas que garantizan la confidencialidad e integridad de la información transmitida. No obstante, debe tenerse en consideración que no todos los algoritmos admitidos por Microsoft son seguros y, por lo tanto, no serían compatibles con la seguridad planteada a través del Esquema Nacional de Seguridad. La política de seguridad de dominio para la categoría básica presenta una implementación de mínimos adecuados con los requisitos de seguridad. No obstante, las pruebas efectuadas en laboratorio han permitido determinar que el empleo de determinados clientes o servidores Linux, o bien la integración con sistemas operativos Microsoft ya obsoletos, pudiera ser incompatible con la configuración establecida.

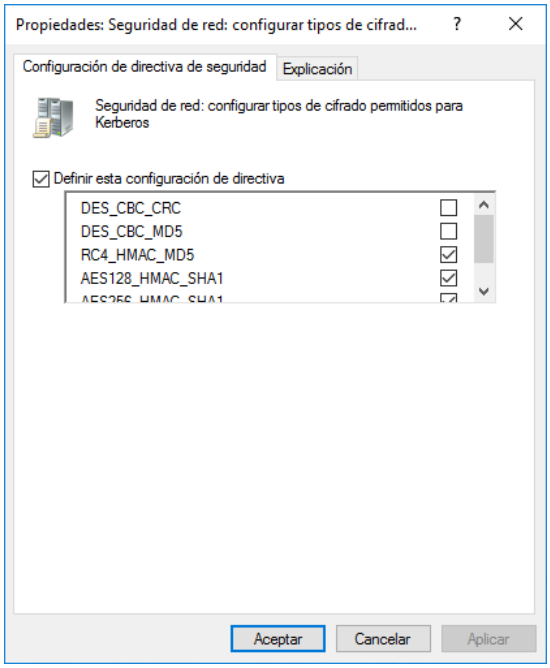
También pudieran darse problemas de comunicación ante determinadas relaciones entre diferentes árboles de un mismo bosque que han ido evolucionando desde dominios Windows NT, Windows 2000, Windows 2003 o Windows 2008.

Nota: Tenga en consideración que Windows Server 2016 ya no está soportado para trabajar a nivel funcional de Windows Server 2003, por lo que deberá actualizar su infraestructura para que el nivel funcional sea superior a 2003.

En caso de identificar problemas de validación de equipos previos a Windows XP o equipos no Microsoft, o bien entre dominio o árboles de un mismo bosque cuando ponga en producción la política de dominio “CCN-STIC-570A ENS incremental Dominio categoria basica”, se deberá realizar una modificación sobre la misma.

Paso	Descripción
68.	Para evaluar y realizar la modificación oportuna inicie la herramienta de “Administración de directivas de grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**

Paso	Descripción
69.	Edite el objeto de GPO “CCN-STIC-570A ENS incremental Dominio categoria basica”. Para ello seleccione dicha política y seleccione la opción “Editar…”. 
70.	Despliegue la política y sitúese en la siguiente ruta: **“Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**
71.	Identifique la directiva “Seguridad de red: configurar tipos de cifrado permitidos para Kerberos”. 

Paso	Descripción
72.	Edítela pulsando doble clic sobre la misma. La configuración predeterminada de seguridad para el cumplimiento de ENS en su categoría básica, es la siguiente. 
73.	Active el resto de opciones pulsando sobre los recuadros que no están marcados y cierre la política mediante el botón “Aceptar”.
74.	Aplique, a posteriori, la nueva configuración para evaluar si se han resuelto las incidencias identificadas. **Nota:** Debe tener en consideración que si ha implementado algoritmos de seguridad alternativos a los propuestos en la configuración deseada de esta guía, se encuentra por debajo de los requerimientos de seguridad actuales. Debería evaluar a qué se deben dichas incidencias y resolverlas para volver a un estado de seguridad adecuado. Es factible que los procesos de autenticación Kerberos para determinados sistemas requieran de algoritmos débiles y pueda encontrarse ante riesgos de seguridad significativos para la organización exponiéndose, por ejemplo, a ataques de tipo *man in the middle* contra los procesos de autenticación en el dominio.

ANEXO A.2.2. LISTA DE COMPROBACIÓN DE WINDOWS SERVER 2016 COMO CONTROLADOR DE DOMINIO PARA LA CATEGORÍA BÁSICA

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía “ANEXO A.2.1 GUÍA PASO A PASO CONTROLADOR DE DOMINIO QUE LE SEA DE APLICACIÓN LA CATEGORÍA BÁSICA”.

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los dominios y servidores Windows Server 2016 con implementación de seguridad de categoría básica del ENS.

Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán

disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador del dominio. Las consolas y herramientas que se utilizarán son las siguientes:

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

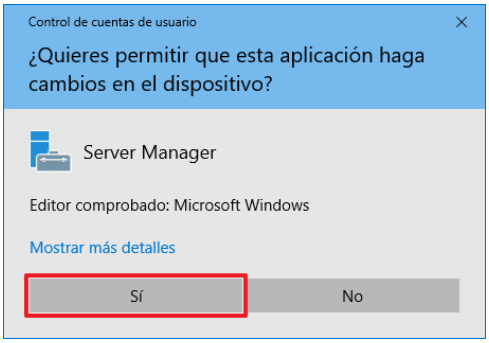
b) Conjunto resultante de directivas (rsop.msc).

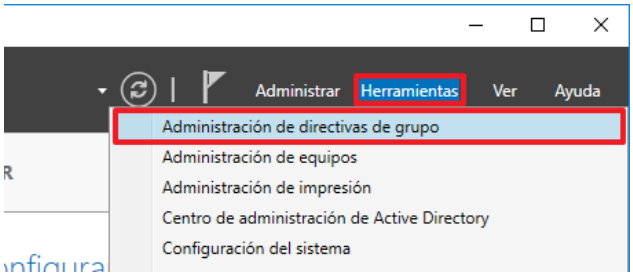
c) Consola de servicios (services.msc).

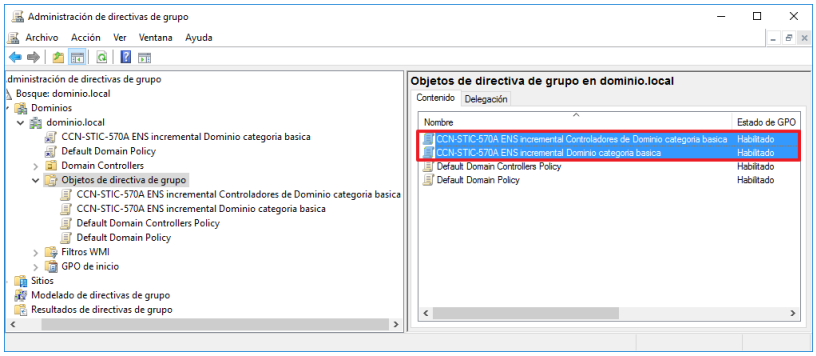
d) Editor de registro (regedit.exe).

e) Explorador de Archivos (explorer.exe).

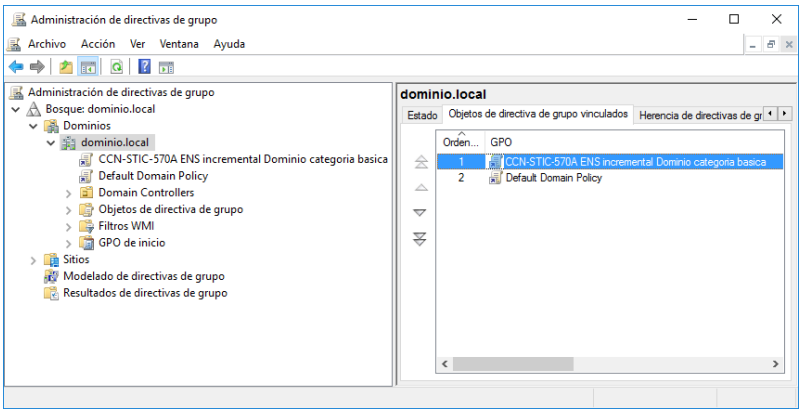
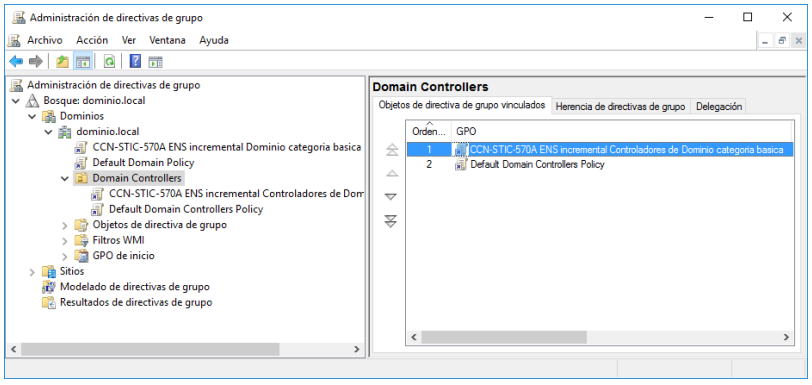
f) Usuarios y equipos de Active Directory (dsa.msc).

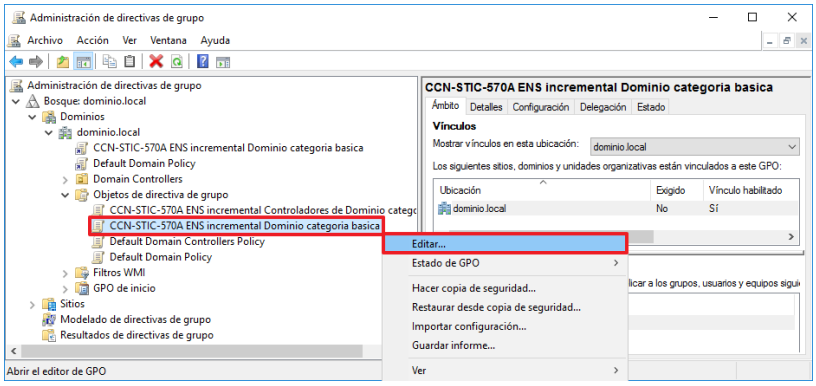
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor".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

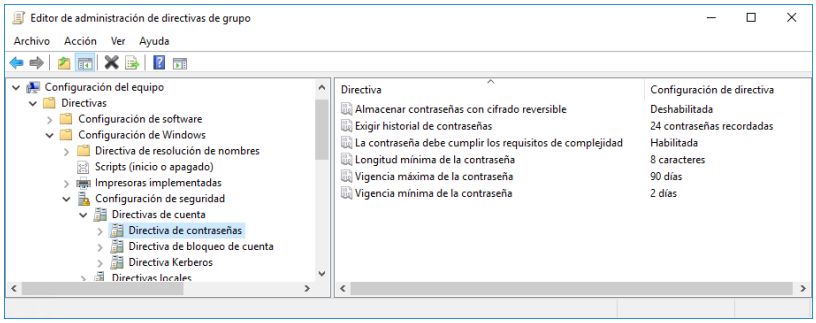
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>2. Verifique que los objetos de directivas de grupo han sido creados y están habilitados.</td><td></td><td>
Ejecute la herramienta “Administrador de directivas de grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione:
“Herramientas → Administración de directivas de grupo”


Dentro de la consola diríjase a los “Objetos de directiva de grupo”:
“Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo”
Verifique que están creados los dos objetos de directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica” y “CCN-STIC-570A ENS incremental Dominio categoria basica”, y que en la columna “Estado de GPO” figuran como habilitadas.


<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica</td><td>Habilitado</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS incremental Dominio categoria basica</td><td>Habilitado</td><td></td></tr>
</table>
</td></tr>
</table>

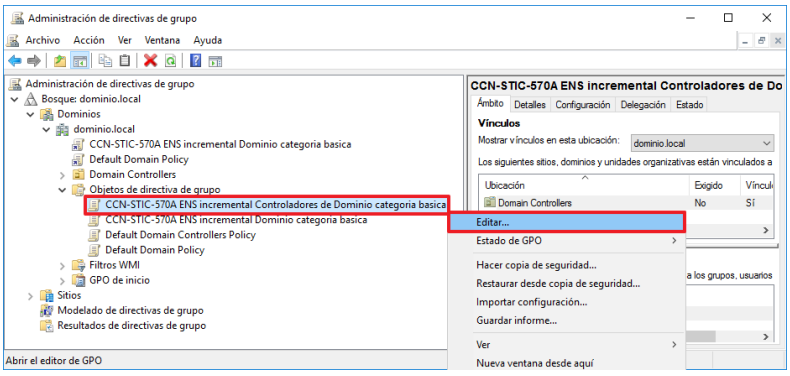
Comprobación	OK/NOK	Cómo hacerlo
3. Verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Dominio categoria basica” aplica a todos los objetos del dominio y ocupa el primer lugar en el orden de vinculación.		En el árbol de la izquierda sitúese sobre el dominio desde: **“Bosque: [Su Bosque] → Dominios → [Su Dominio]”** **En la pestaña “Objetos de Directiva de grupo vinculados”** verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Dominio categoria basica” figura en el panel de la derecha y ocupa el primer lugar en la columna “Orden de Vínculos”. 
4. Verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Controladores de dominio categoria basica” aplica a todos los objetos del contenedor “Domain Controllers” y ocupa el primer lugar en el orden de vinculación.		En el árbol de la izquierda sitúese sobre el contenedor “Domain Controllers” desde: **“Bosque: [Su Bosque] → Dominios → [Su Dominio] → Domain Controllers”** En la pestaña “Objetos de Directiva de grupo vinculados” verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Controladores de dominio categoria basica” figura en el panel de la derecha y ocupa el primer lugar en la columna “Orden de Vínculos”. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>5. Verifique la directiva de contraseñas en el objeto de directiva “CCN-STIC-570A ENS incremental Dominio categoria basica”.</td><td></td><td>
En el “Administrador de Directivas de Grupo” pulse el botón derecho del ratón sobre la directiva desde:
“Bosque: [Su Bosque] → Dominios → [Su Dominio] → CCN-STIC-570A ENS incremental Dominio categoria basica”
Seleccione la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.


Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de contraseñas”


<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Almacenar contraseñas usando cifrado reversible</td><td>Deshabilitada</td><td></td></tr>
<tr><td>Exigir historial de contraseñas</td><td>24 contraseñas recordadas</td><td></td></tr>
<tr><td>Las contraseñas deben cumplir los requisitos de complejidad</td><td>Habilitada</td><td></td></tr>
<tr><td>Longitud mínima de la contraseña</td><td>8 caracteres</td><td></td></tr>
<tr><td>Vigencia máxima de la contraseña</td><td>90 días</td><td></td></tr>
<tr><td>Vigencia mínima de la contraseña</td><td>2 días</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td rowspan="5">6. Verifique las directivas de bloqueo de cuenta de la directiva de grupo “CCN-STIC-570A ENS incremental Dominio categoria basica”.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de bloqueo de cuenta”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Duración del bloqueo de cuenta</td><td>30 minutos</td><td></td></tr>
<tr><td colspan="2">Restablecer recuentos de bloqueo de cuenta tras</td><td>30 minutos</td><td></td></tr>
<tr><td colspan="2">Umbral de bloqueo de cuenta</td><td>8 intentos de inicio de sesión no válidos</td><td></td></tr>
<tr><td rowspan="6">7. Verifique las directivas Kerberos en la directiva de grupo “CCN-STIC-570A ENS incremental Dominio categoria basica”.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva Kerberos”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Aplicar restricciones de inicio de sesión de usuario</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Tolerancia máxima para la sincronización de los relojes de los equipos</td><td>10 minutos</td><td></td></tr>
<tr><td colspan="2">Vigencia máxima de renovación de vales de usuario</td><td>4 días</td><td></td></tr>
<tr><td colspan="2">Vigencia máxima del vale de servicio</td><td>480 minutos</td><td></td></tr>
<tr><td colspan="2">Vigencia máxima del vale de usuario</td><td>8 horas</td><td></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>8. Verifique las opciones de seguridad de la directiva de grupo “CCN-STIC-570A ENS incremental Dominio categoria basica”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas Locales → Opciones de seguridad”
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Acceso de red: permitir traducción SID/nombre anónima</td><td>Deshabilitada</td><td></td></tr>
<tr><td>Seguridad de red: configurar tipos de cifrado permitidos para Kerberos</td><td>DES_CBC_CRC (Deshabilitado)
DES_CBC_MD5 (Deshabilitado)
RC4_HMAC_MD5 (Habilitado)
AES128_HMAC_SHA1 (Habilitado)
AES256_HMAC_SHA1 (Habilitado)
Tipos de cifrado futuros (Habilitado)</td><td></td></tr>
</table></td></tr>
<tr><td>9. Verifique las directivas de auditoría en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica”.</td><td></td><td>En el “Administrador de Directivas de Grupo” pulse el botón derecho del ratón sobre la directiva desde:
“Bosque: [Su Bosque] → Dominios → [Su Dominio] → Domain Controllers → CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica”
Seleccione la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 

Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="10"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Auditar el acceso a objetos</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td colspan="2">Auditar el acceso del servicio de directorio</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td colspan="2">Auditar el cambio de directivas</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td colspan="2">Auditar el seguimiento de procesos</td><td>Sin auditoría</td><td></td></tr>
<tr><td colspan="2">Auditar el uso de privilegios</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td colspan="2">Auditar eventos de inicio de sesión</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td colspan="2">Auditar eventos de inicio de sesión de cuenta</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td colspan="2">Auditar eventos del sistema</td><td>Correcto</td><td></td></tr>
<tr><td colspan="2">Auditar la administración de cuentas</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td rowspan="11">10. Verifique la asignación de derechos de usuario en la directiva “CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica”.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Administrar registro de seguridad y auditoría</td><td>Administradores</td><td></td></tr>
<tr><td colspan="2">Agregar estaciones de trabajo al dominio</td><td>Administradores</td><td></td></tr>
<tr><td colspan="2">Ajustar las cuotas de la memoria para un proceso</td><td>Administradores, SERVICIO LOCAL, Servicio de red</td><td></td></tr>
<tr><td colspan="2">Apagar el sistema</td><td>Administradores</td><td></td></tr>
<tr><td colspan="2">Aumentar el espacio de trabajo de un proceso</td><td>Administradores, SERVICIO LOCAL</td><td></td></tr>
<tr><td colspan="2">Aumentar prioridad de programación</td><td>Administradores</td><td></td></tr>
<tr><td colspan="2">Bloquear páginas en la memoria</td><td>Administradores</td><td></td></tr>
<tr><td colspan="2">Cambiar la hora del sistema</td><td>SERVICIO LOCAL, Administradores</td><td></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Cambiar la zona horaria	SERVICIO LOCAL, Administradores	
		Cargar y descargar controladores de dispositivo	Administradores	
		Crear objetos globales	Administradores, SERVICIO, SERVICIO LOCAL, Servicio de red	
		Crear un archivo de paginación	Administradores	
		Crear vínculos simbólicos	Administradores	
		Denegar el acceso desde la red a este equipo	ANONYMOUS LOGON, Invitados	
		Denegar el inicio de sesión como servicio	Invitados	
		Denegar el inicio de sesión como trabajo por lotes	Invitados	
		Denegar el inicio de sesión localmente	Invitados	
		Denegar inicio de sesión a través de Servicios de Terminal Server	Invitados	
		Forzar cierre desde un sistema remoto	Administradores	
		Generar auditorías de seguridad	SERVICIO LOCAL, Servicio de red	
		Generar perfiles de un solo proceso	Administradores	
		Generar perfiles del rendimiento del sistema	Administradores	
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	Administradores	
		Hacer copias de seguridad de archivos y directorios	Administradores, Operadores de copia de seguridad	
		Modificar la etiqueta de un objeto	Administradores	
		Modificar valores de entorno firmware	Administradores	
		Permitir el inicio de sesión local	Administradores	
		Quitar equipo de la estación de acoplamiento	Administradores	
		Realizar tareas de mantenimiento de volumen	Administradores	
		Reemplazar un símbolo (token) de nivel de proceso	SERVICIO LOCAL, Servicio de red	
		Restaurar archivos y directorios	Administradores	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="4"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Suplantar a un cliente tras la autenticación</td><td>Administradores, SERVICIO, SERVICIO LOCAL, Servicio de red</td><td></td></tr>
<tr><td colspan="2">Tener acceso a este equipo desde la red</td><td>Administradores, Usuarios autentificados, ENTERPRISE DOMAIN CONTROLLERS</td><td></td></tr>
<tr><td colspan="2">Tomar posesión de archivos y otros objetos</td><td>Administradores</td><td></td></tr>
<tr><td rowspan="6">11. Verifique las opciones de seguridad en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica”.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Acceso a redes: modelo de seguridad y uso compartido para cuentas locales</td><td>Clásico: usuarios locales se autentican con credenciales propias</td><td></td></tr>
<tr><td colspan="2">Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos</td><td>Deshabilitada</td><td></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos	Habilitada	
		Acceso a redes: rutas del Registro accesibles remotamente	System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, Software\Microsoft\Windows NT\CurrentVersion	
		Acceso a redes: rutas y subrutas del Registro accesibles remotamente	Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib, System\CurrentControlSet\Services\SysmonLog	
		Acceso a red: permitir traducción SID/nombre anónima	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Apagado: permitir apagar el sistema sin tener que iniciar sesión	Deshabilitada	
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitada	
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitada	
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada	
		Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Habilitada	
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitada	
		Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador	Pedir consentimiento en el escritorio seguro	
		Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar	Pedir credenciales en el escritorio seguro	
		Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación	Habilitada	
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitada	
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Controlador de dominio: no permitir los cambios de contraseña de cuenta de equipo	Deshabilitada	
		Criptografía de sistema: forzar la protección con claves seguras para las claves de usuario almacenadas en el equipo	El usuario debe escribir una contraseña cada vez que use una clave.	
		Cuentas: estado de la cuenta de invitado	Deshabilitada	
		Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitada	
		DCOM: restricciones de acceso al equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)	O:BAG:BAD:(A;;CCDCLC;;;AU)(A;;CCDCLC;;;S-1-5-32-562)	
		DCOM: restricciones de inicio al equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)	O:BAG:BAD:(A;;CCDCLCSWRP;;;BA)(A;;CSW;;;AU)(A;;CCDCLCSWRP;;;S-1-5-32-562)	
		Dispositivos: permitir formatear y expulsar medios extraíbles	Administradores y usuarios avanzados	
		Dispositivos: restringir el acceso a disquetes sólo al usuario con sesión iniciada localmente	Habilitada	
		Dispositivos: restringir el acceso al CD-ROM sólo al usuario con sesión iniciada localmente	Habilitada	
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Inicio de sesión interactivo: mostrar información del usuario cuando se bloquee la sesión	No mostrar la información del usuario	
		Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr	Deshabilitada	
		Inicio de sesión interactivo: número de inicios de sesión anteriores que se almacenarán en caché (si el controlador de dominio no está disponible)	1 inicios de sesión	
		Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire	14 días	
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	
		Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitada	
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitada	
		Miembro de dominio: duración máxima de contraseña de cuenta de equipo	30 días	
		Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	
		Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitada	
		Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitada	
		Seguridad de red: nivel de autenticación de LAN Manager	Enviar sólo respuesta NTLMv2 y rechazar LM	
		Directiva	Valor	OK/NOK

Comprobación	OK/NOK	Cómo hacerlo		
		Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada	
		Seguridad de red: permitir que LocalSystem use la identidad del equipo para NTLM	Habilitada	
		Seguridad de red: permitir retroceso a sesión NULL de LocalSystem	Deshabilitada	
		Seguridad de red: permitir solicitudes de autenticación PKU2U a este equipo para usar identidades en Internet.	Deshabilitada	
		Seguridad de red: restringir NTLM: auditar el tráfico NTLM entrante	Habilitar la auditoría para todas las cuentas	
		Seguridad de red: restringir NTLM: auditar la autenticación NTLM en este dominio	Habilitar todo	
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitada	
		Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor	Aceptar si lo proporciona el cliente	
		Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión	30 minutos	
12. Verifique el registro de eventos en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica”.		Seleccione el siguiente nodo. **“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro de Eventos”**		

Comprobación	OK/NOK	Cómo hacerlo

Directiva	Valor	OK/NOK
Evitar que el grupo de invitados locales tenga acceso al registro de aplicaciones	Habilitada	
Evitar que el grupo de invitados locales tenga acceso al registro de seguridad	Habilitada	
Evitar que el grupo de invitados locales tenga acceso al registro del sistema	Habilitada	
Método de retención del registro de la aplicación	Según se necesite	
Método de retención del registro de seguridad	Según se necesite	
Método de retención del registro del sistema	Según se necesite	
Tamaño máximo del registro de la aplicación	32768 kilobytes	
Tamaño máximo del registro de seguridad	163840 kilobytes	
Tamaño máximo del registro del sistema	32768 kilobytes	

13. Verifique los servicios del sistema en la directiva de grupo "CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica".

Seleccione el siguiente nodo.
"Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"

Nota: Dependiendo de los servicios que estén instalados en el equipo, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales (antivirus, etc.).
En la siguiente tabla se muestran el nombre largo y el nombre corto para cada servicio. En la ventana del editor de administración de directivas de grupo sólo aparecerá uno de los dos: el nombre largo si el servicio está instalado en el sistema o el nombre corto si no lo está.
Además, deberá tener en cuenta que los números existentes en algunos servicios son aleatorios y cambian en cada equipo.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado	
Administración de aplicaciones	AppMgmt	Manual	Configurado	

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK

Comprobación	OK/NOK	Cómo hacerlo			
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado		
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado		
Administración remota de Windows (WS-Management)	WinRM	Automático	Configurado		
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado		
Administrador de conexiones de acceso remoto	RasMan	Manual	Configurado		
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado		
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado		
Administrador de credenciales	VaultSvc	Manual	Configurado		
Administrador de cuentas de seguridad	SamSs	Automático	Configurado		
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado		
Administrador de sesión local	LSM	Automático	Configurado		
Administrador de usuarios	UserManager	Automático	Configurado		
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado		
Agente de conexión de red	NcbService	Manual	Configurado		
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado		
Agente de directiva IPsec	PolicyAgent	Manual	Configurado		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**	
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado		
Aislamiento de claves CNG	KeyIso	Manual	Configurado		
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado		
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado		
Aplicación auxiliar IP	iphlpsvc	Automático	Configurado		
Aplicación del sistema COM+	COMSysApp	Manual	Configurado		
Archivos sin conexión	CscService	Deshabilitado	Configurado		
Asignador de detección de topologías de nivel de vínculo	lltdsvc	Manual	Configurado		
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado		
Asistente para la conectividad de red	NcaSvc	Manual	Configurado		
Audio de Windows	Audiosrv	Manual	Configurado		
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Deshabilitado	Configurado		
Ayudante especial de la consola de administración	sacsvr	Manual	Configurado		
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado		
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado		
CDPUserSvc	CDPUserSvc	Automático	Configurado		
Centro de distribución de claves Kerberos	Kdc	Automático	Configurado		
Cliente de directiva de grupo	gpsvc	Automático	Configurado		
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático	Configurado		
Cliente DHCP	Dhcp	Automático	Configurado		
Cliente DNS	Dnscache	Automático	Configurado		
Cola de impresión	Spooler	Automático	Configurado		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**	
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Manual	Configurado		
Comprobador puntual	svsvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado	
Conexiones de red	Netman	Manual	Configurado	
Configuración automática de redes cableadas	dot3svc	Manual	Configurado	
Configuración de Escritorio remoto	SessionEnv	Manual	Configurado	
Conjunto resultante de proveedor de directivas	RSoPProv	Manual	Configurado	
Contenedor de Microsoft Passport	NgcCtnrSvc	Manual	Configurado	
Coordinador de transacciones distribuidas	MSDTC	Automático	Configurado	
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado	
DataCollectionPublishingService	DcpSvc	Manual	Configurado	
Datos de contactos	PimIndexMaintenanceSvc	Manual	Configurado	
Detección de hardware shell	ShellHWDetection	Deshabilitado	Configurado	
Detección de servicios interactivos	UI0Detect	Manual	Configurado	
Detección SSDP	SSDPSRV	Deshabilitado	Configurado	
Directiva de extracción de tarjetas inteligentes	SCPolicySvc	Manual	Configurado	
Disco virtual	vds	Manual	Configurado	
Dispositivo host de UPnP	upnphost	Manual	Configurado	
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado	
dmwappushsvc	dmwappushservice	Deshabilitado	Configurado	
Energía	Power	Automático	Configurado	
Enrutamiento y acceso remoto	RemoteAccess	Deshabilitado	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Espacio de nombres DFS	Dfs	Automático	Configurado	
Estación de trabajo	LanmanWorkstation	Automático	Configurado	
Eventos de adquisición de imágenes estáticas	WiaRpc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Examinador de equipos	Browser	Deshabilitado	Configurado	
Experiencia de calidad de audio y vídeo de Windows (qWave)	QWAVE	Deshabilitado	Configurado	
Extensiones y notificaciones de impresora	PrintNotify	Manual	Configurado	
Firewall de Windows	MpsSvc	Automático	Configurado	
Hora de Windows	W32Time	Automático	Configurado	
Host de proveedor de detección de función	fdPHost	Deshabilitado	Configurado	
Host de sistema de diagnóstico	WdiSystemHost	Deshabilitado	Configurado	
Host del servicio de diagnóstico	WdiServiceHost	Deshabilitado	Configurado	
Identidad de aplicación	AppIDSvc	Manual	Configurado	
Información de la aplicación	Appinfo	Manual	Configurado	
Iniciador de procesos de servidor DCOM	DcomLaunch	Automático	Configurado	
Inicio de sesión secundario	seclogon	Deshabilitado	Configurado	
Instalador de ActiveX (AxInstSV)	AxInstSV	Manual	Configurado	
Instalador de módulos de Windows	TrustedInstaller	Manual	Configurado	
Instantáneas de volumen	VSS	Manual	Configurado	
Instrumental de administración de Windows	Winmgmt	Automático	Configurado	
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado	
KTMRM para DTC (Coordinador de transacciones distribuidas)	KtmRm	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Llamada a procedimiento remoto (RPC)	RpcSs	Automático	Configurado	
Mensajería entre sitios	IsmServ	Automático	Configurado	
Microsoft App-V Client	AppVClient	Deshabilitado	Configurado	
Microsoft Passport	NgcSvc	Manual	Configurado	
Modo incrustado	embeddedmode	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Módulos de creación de claves de IPsec para IKE y AuthIP		IKEEXT	Manual	Configurado	
Motor de filtrado de base		BFE	Automático	Configurado	
Net Logon		Netlogon	Automático	Configurado	
Optimizar unidades		defragsvc	Manual	Configurado	
Partida guardada en Xbox Live		XblGameSave	Deshabilitado	Configurado	
Plug and Play		PlugPlay	Manual	Configurado	
Preparación de aplicaciones		AppReadiness	Manual	Configurado	
Programador de tareas		Schedule	Automático	Configurado	
Propagación de certificados		CertPropSvc	Manual	Configurado	
Protección de software		sppsvc	Automático	Configurado	
Protocolo de autenticación extensible		Eaphost	Manual	Configurado	
Proveedor de instantáneas de software de Microsoft		swprv	Manual	Configurado	
Publicación de recurso de detección de función		FDResPub	Deshabilitado	Configurado	
Reconoc. ubicación de red		NlaSvc	Automático	Configurado	
Recopilador de eventos de Windows		Wecsvc	Manual	Configurado	
Redirector de puerto en modo usuario de Servicios de Escritorio remoto		UmRdpService	Manual	Configurado	
Registro de eventos de Windows		EventLog	Automático	Configurado	
Registro remoto		RemoteRegistry	Automático	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Registros y alertas de rendimiento		pla	Manual	Configurado	
Replicación de archivos		NtFrs	Deshabilitado	Configurado	
Replicación DFS		DFSR	Automático	Configurado	
Servicio Asistente para la compatibilidad de programas		PcaSvc	Automático	Configurado	
Servicio biométrico de		WbioSrvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Windows					
Servicio de actualizaciones Orchestrator para Windows Update		UsoSvc	Manual	Configurado	
Servicio de administración de aplicaciones de empresa		EntAppSvc	Manual	Configurado	
Servicio de administración de radio		RmSvc	Manual	Configurado	
Servicio de administrador de licencias de Windows		LicenseManager	Manual	Configurado	
Servicio de almacenamiento		StorSvc	Manual	Configurado	
Servicio de asociación de dispositivos		DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows		FontCache	Deshabilitado	Configurado	
Servicio de cierre de invitado de Hyper-V		vmicshutdown	Manual	Configurado	
Servicio de compatibilidad con Bluetooth		bthserv	Manual	Configurado	
Servicio de configuración de red		NetSetupSvc	Manual	Configurado	
Servicio de datos del sensor		SensorDataService	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP		WinHttpAutoProxySvc	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de directivas de diagnóstico		DPS	Deshabilitado	Configurado	
Servicio de dispositivo de interfaz humana		hidserv	Manual	Configurado	
Servicio de distribución de clave de Microsoft		KdsSvc	Manual	Configurado	
Servicio de enrutador de AllJoyn		AJRouter	Deshabilitado	Configurado	
Servicio de		ScDeviceEnum	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
enumeración de dispositivos de tarjeta inteligente					
Servicio de geolocalización		lfsvc	Manual	Configurado	
Servicio de host HV		HvHost	Manual	Configurado	
Servicio de implementación de AppX (AppXSVC)		AppXSvc	Manual	Configurado	
Servicio de infraestructura de tareas en segundo plano		BrokerInfrastructure	Automático	Configurado	
Servicio de inscripción de administración de dispositivos		DmEnrollmentSvc	Manual	Configurado	
Servicio de inspección de red de Windows Defender		WdNisSvc	Manual	Configurado	
Servicio de instalación de dispositivos		DeviceInstall	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V		vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V		vmicheartbeat	Manual	Configurado	
Servicio de licencia de cliente (ClipSVC)		ClipSVC	Manual	Configurado	
Servicio de lista de redes		netprofm	Manual	Configurado	
Servicio de notificación de eventos de sistema		SENS	Automático	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de Panel de escritura a mano y teclado táctil		TabletInputService	Deshabilitado	Configurado	
Servicio de perfil de usuario		ProfSvc	Automático	Configurado	
Servicio de plataforma de dispositivos conectados		CDPSvc	Automático	Configurado	
Servicio de protocolo de túnel de sockets seguros		SstpSvc	Manual	Configurado	
Servicio de puerta de		ALG	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
enlace de nivel de aplicación				
Servicio de registro de acceso de usuarios	UALSVC	Automático	Configurado	
Servicio de repositorio de estado	StateRepository	Manual	Configurado	
Servicio de sensores	SensorService	Manual	Configurado	
Servicio de servidor proxy KDC (KPS)	KPSSVC	Manual	Configurado	
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado	
Servicio de supervisión de licencias de Windows	WLMS	Automático	Configurado	
Servicio de supervisión de sensores	SensrSvc	Manual	Configurado	
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Manual	Configurado	
Servicio de uso compartido de datos	DsSvc	Manual	Configurado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Deshabilitado	Configurado	
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Manual	Configurado	

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual	Configurado	
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado	
Servicio de Windows Defender	WinDefend	Automático	Configurado	
Servicio de Windows Insider	wisvc	Manual	Configurado	
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Manual	Configurado	
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado	
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Manual	Configurado	
Servicio FrameServer de la Cámara de Windows	FrameServer	Manual	Configurado	
Servicio host de proveedor de cifrado de Windows	WEPHOSTSVC	Manual	Configurado	
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado	
Servicio Interfaz de almacenamiento en red	nsi	Automático	Configurado	
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado	
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standardcollector.service	Manual	Configurado	
Servicio telefónico	PhoneSvc	Manual	Configurado	
Servicios de cifrado	CryptSvc	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicios de dominio de Active Directory	NTDS	Automático	Configurado	
Servicios de Escritorio remoto	TermService	Manual	Configurado	
Servicios web de Active Directory	ADWS	Automático	Configurado	
Servidor	LanmanServer	Automático	Configurado	
Servidor de roles de DS	DsRoleSvc	Manual	Configurado	
Servidor del modelo de datos del mosaico	tiledatamodelsvc	Automático	Configurado	
Servidor DNS	DNS	Automático	Configurado	
Sincronizar host	OneSyncSvc	Automático	Configurado	
Sistema de cifrado de archivos (EFS)	EFS	Manual	Configurado	
Sistema de eventos COM+	EventSystem	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
SMP de Espacios de almacenamiento de Microsoft		smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V		vmicvss	Manual	Configurado	
Superfetch		SysMain	Manual	Configurado	
Tarjeta inteligente		SCardSvr	Deshabilitado	Configurado	
Telefonía		TapiSrv	Deshabilitado	Configurado	
Telemetría y experiencias del usuario conectado		DiagTrack	Automático	Configurado	
Temas		Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)		RpcLocator	Manual	Configurado	
WalletService		WalletService	Manual	Configurado	
Windows Driver Foundation - User-mode Driver Framework		wudfsvc	Manual	Configurado	
Windows Installer		msiserver	Manual	Configurado	
Windows Search		WSearch	Deshabilitado	Configurado	
Windows Update		wuauserv	Manual	Configurado	

14. Verifique los permisos de valores de registro de la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica”.

Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro”

Nota: Para verificar los permisos de la entrada de registro, deberá pulsar doble clic sobre la entrada **“MACHINES → SOFTWARE → Microsoft → Windows → CurrentVersion → Installer”** y pulsar sobre el botón "Modificar seguridad...".

Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".

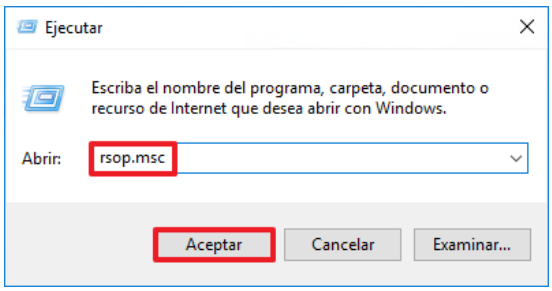
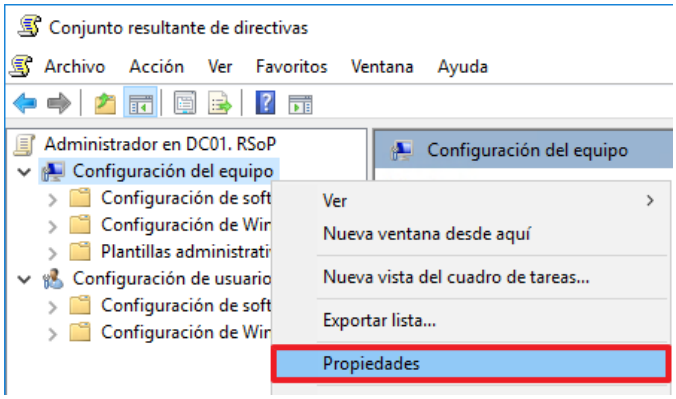
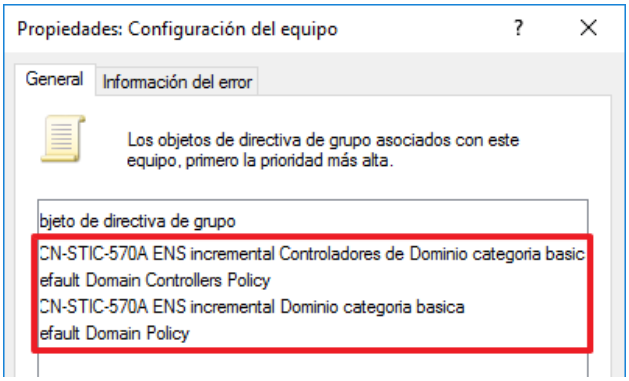
Directiva	Valor	OK/NOK
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer	Administradores: Control Total SYSTEM: Control Total Usuarios: Leer	

Comprobación	OK/NOK	Cómo hacerlo
15. Verifique los valores del sistema de archivos de la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica”.		Seleccione el siguiente nodo. **“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de Archivos”** **Nota:** Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción “Propiedades” del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...". Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		**Usuario**	**Permiso**	**OK/NOK**
%SystemRoot%\Registration		Administrador	Control total	
		System	Control total	
		Usuario	Leer y ejecutar	
%SystemRoot%\repair		Administrador	Control total	
		System	Control total	
%SystemRoot%\security		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\cacls.exe		Administrador	Control total	
		System	Control total	
SystemRoot%\system32\clip.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\ras		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\rasadhlp.dll		Administrador	Control total	
%SystemRoot%\system32\rasauto.dll		Administrador	Control total	
%SystemRoot%\system32\rasautou.exe		Administrador	Control total	
%SystemRoot%\system32\raschap.dll		Administrador	Control total	
%SystemRoot%\system32\rasctrnm.h		Administrador	Control total	
%SystemRoot%\system32\rasctrs.dll		Administrador	Control total	
%SystemRoot%\system32\rasctrs.ini		Administrador	Control total	
%SystemRoot%\system32\rasdial.exe		Administrador	Control total	
%SystemRoot%\system32\rasmans.dll		Administrador	Control total	
%SystemRoot%\system32\rasmontr.dll		Administrador	Control total	
%SystemRoot%\system32\rasphone.exe		Administrador	Control total	
%SystemRoot%\system32\rasppp.dll		Administrador	Control total	
%SystemRoot%\system32\rastapi.dll		Administrador	Control total	
%SystemRoot%\system32\rastls.dll		Administrador	Control total	
%SystemRoot%\system32\runonce.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\secedit.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\telnet.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\tftp.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\tracert.exe		Administrador	Control total	
		System	Control total	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td rowspan="4">16. Verifique que está bloqueada la ejecución del Almacén digital en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Almacén Digital”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">No permitir que se ejecute el Almacén digital</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="4">17. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Informe de errores de Windows”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Deshabilitar el informe de errores de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">No enviar datos adicionales</td><td>Habilitada</td><td></td></tr>
</table>

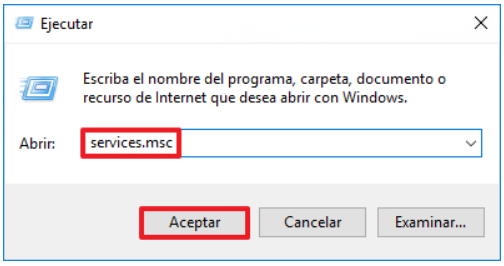
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>18. Verifique configuración de la comunicación de Internet en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Desactivar informe de errores de reconocimiento de escritura a mano</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el Programa para la mejora de la experiencia del usuario de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar los vínculos “Events.asp” del Visor de eventos</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el contenido “¿Sabía que…?” del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la búsqueda en Microsoft Knowledge Base del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el informe de errores de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la actualización de archivos de contenido del Asistente para búsqueda</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el acceso a la Tienda</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la tarea de imágenes “Pedir copias fotográficas”</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger</td><td>Habilitada</td><td></td></tr>
</table>
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
19. Verifique que el equipo ha recibido las directivas de grupo CC-STIC-570A ENS incremental Dominio categoria basica y CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica		Ejecute la consola de administración "Conjunto resultante de directivas" (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → rsop.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" para continuar.  Seleccione en ella la rama "Configuración del equipo", márquela con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la figura:  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", resaltada en la siguiente figura:  Verifique que en dicha sección aparecen listados, y por ese orden, los objetos de directiva de grupo que se indican en la siguiente tabla:

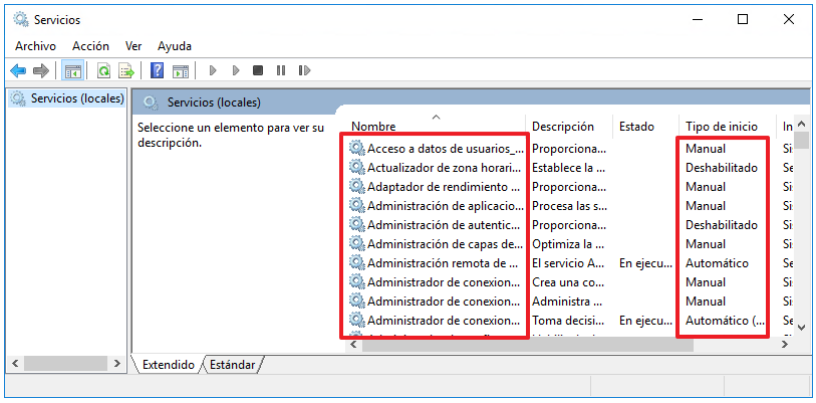
Comprobación	OK/NOK	Cómo hacerlo
	Objeto de directiva de grupo	OK/NOK
	CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica	
	Default Domain Controllers Policy	
	CCN-STIC-570A ENS incremental Dominio categoria basica	
	Default Domain Policy	

20. Verifique que los servicios del sistema están correctamente configurados

Usando la consola de servicios (el sistema solicitará elevación de privilegios):
"Tecla Windows+R → services.msc"
El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" para continuar.



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



Nota: Dependiendo del equipo, es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales (antivirus, etc.).

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado	
Administración de aplicaciones	AppMgmt	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado	
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado	
Administración remota de Windows (WS-Management)	WinRM	Automático	Configurado	
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado	
Administrador de conexiones de acceso remoto	RasMan	Manual	Configurado	
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado	
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado	
Administrador de credenciales	VaultSvc	Manual	Configurado	
Administrador de cuentas de seguridad	SamSs	Automático	Configurado	
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado	
Administrador de sesión local	LSM	Automático	Configurado	
Administrador de usuarios	UserManager	Automático	Configurado	
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado	
Agente de conexión de red	NcbService	Manual	Configurado	
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado	
Agente de directiva IPsec	PolicyAgent	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Espacio de nombres	Dfs	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
DFS					
Estación de trabajo		LanmanWorkstation	Automático	Configurado	
Eventos de adquisición de imágenes estáticas		WiaRpc	Manual	Configurado	
Examinador de equipos		Browser	Deshabilitado	Configurado	
Experiencia de calidad de audio y vídeo de Windows (qWave)		QWAVE	Deshabilitado	Configurado	
Extensiones y notificaciones de impresora		PrintNotify	Manual	Configurado	
Firewall de Windows		MpsSvc	Automático	Configurado	
Hora de Windows		W32Time	Automático	Configurado	
Host de proveedor de detección de función		fdPHost	Deshabilitado	Configurado	
Host de sistema de diagnóstico		WdiSystemHost	Deshabilitado	Configurado	
Host del servicio de diagnóstico		WdiServiceHost	Deshabilitado	Configurado	
Identidad de aplicación		AppIDSvc	Manual	Configurado	
Información de la aplicación		Appinfo	Manual	Configurado	
Iniciador de procesos de servidor DCOM		DcomLaunch	Automático	Configurado	
Inicio de sesión secundario		seclogon	Deshabilitado	Configurado	
Instalador de ActiveX (AxInstSV)		AxInstSV	Manual	Configurado	
Instalador de módulos de Windows		TrustedInstaller	Manual	Configurado	
Instantáneas de volumen		VSS	Manual	Configurado	
Instrumental de administración de Windows		Winmgmt	Automático	Configurado	
Interfaz de servicio invitado de Hyper-V		vmicguestinterface	Manual	Configurado	
KTMRM para DTC (Coordinador de transacciones distribuidas)		KtmRm	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Llamada a procedimiento remoto (RPC)		RpcSs	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Mensajería entre sitios	IsmServ	Automático	Configurado	
Microsoft App-V Client	AppVClient	Deshabilitado	Configurado	
Microsoft Passport	NgcSvc	Manual	Configurado	
Modo incrustado	embeddedmode	Manual	Configurado	
Módulos de creación de claves de IPsec para IKE y AuthIP	IKEEXT	Manual	Configurado	
Motor de filtrado de base	BFE	Automático	Configurado	
Net Logon	Netlogon	Automático	Configurado	
Optimizar unidades	defragsvc	Manual	Configurado	
Partida guardada en Xbox Live	XblGameSave	Deshabilitado	Configurado	
Plug and Play	PlugPlay	Manual	Configurado	
Preparación de aplicaciones	AppReadiness	Manual	Configurado	
Programador de tareas	Schedule	Automático	Configurado	
Propagación de certificados	CertPropSvc	Manual	Configurado	
Protección de software	sppsvc	Automático	Configurado	
Protocolo de autenticación extensible	Eaphost	Manual	Configurado	
Proveedor de instantáneas de software de Microsoft	swprv	Manual	Configurado	
Publicación de recurso de detección de función	FDResPub	Deshabilitado	Configurado	
Reconoc. ubicación de red	NlaSvc	Automático	Configurado	
Recopilador de eventos de Windows	Wecsvc	Manual	Configurado	
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService	Manual	Configurado	
Registro de eventos de Windows	EventLog	Automático	Configurado	
Registro remoto	RemoteRegistry	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Registros y alertas de rendimiento	pla	Manual	Configurado	
Replicación de archivos	NtFrs	Deshabilitado	Configurado	
Replicación DFS	DFSR	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio Asistente para la compatibilidad de programas		PcaSvc	Automático	Configurado	
Servicio biométrico de Windows		WbioSrvc	Manual	Configurado	
Servicio de actualizaciones Orchestrator para Windows Update		UsoSvc	Manual	Configurado	
Servicio de administración de aplicaciones de empresa		EntAppSvc	Manual	Configurado	
Servicio de administración de radio		RmSvc	Manual	Configurado	
Servicio de administrador de licencias de Windows		LicenseManager	Manual	Configurado	
Servicio de almacenamiento		StorSvc	Manual	Configurado	
Servicio de asociación de dispositivos		DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows		FontCache	Deshabilitado	Configurado	
Servicio de cierre de invitado de Hyper-V		vmicshutdown	Manual	Configurado	
Servicio de compatibilidad con Bluetooth		bthserv	Manual	Configurado	
Servicio de configuración de red		NetSetupSvc	Manual	Configurado	
Servicio de datos del sensor		SensorDataService	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP		WinHttpAutoProxySvc	Manual	Configurado	
Servicio de directivas de diagnóstico		DPS	Deshabilitado	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de dispositivo de interfaz humana		hidserv	Manual	Configurado	
Servicio de distribución de clave de Microsoft		KdsSvc	Manual	Configurado	
Servicio de enrutador		AJRouter	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
de AllJoyn					
Servicio de enumeración de dispositivos de tarjeta inteligente		ScDeviceEnum	Manual	Configurado	
Servicio de geolocalización		lfsvc	Manual	Configurado	
Servicio de host HV		HvHost	Manual	Configurado	
Servicio de implementación de AppX (AppXSVC)		AppXSvc	Manual	Configurado	
Servicio de infraestructura de tareas en segundo plano		BrokerInfrastructure	Automático	Configurado	
Servicio de inscripción de administración de dispositivos		DmEnrollmentSvc	Manual	Configurado	
Servicio de inspección de red de Windows Defender		WdNisSvc	Manual	Configurado	
Servicio de instalación de dispositivos		DeviceInstall	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V		vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V		vmicheartbeat	Manual	Configurado	
Servicio de licencia de cliente (ClipSVC)		ClipSVC	Manual	Configurado	
Servicio de lista de redes		netprofm	Manual	Configurado	
Servicio de notificación de eventos de sistema		SENS	Automático	Configurado	
Servicio de Panel de escritura a mano y teclado táctil		TabletInputService	Deshabilitado	Configurado	
Servicio de perfil de usuario		ProfSvc	Automático	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de plataforma de dispositivos conectados		CDPSvc	Automático	Configurado	
Servicio de protocolo de túnel de sockets seguros		SstpSvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio de puerta de enlace de nivel de aplicación	ALG	Manual	Configurado		
Servicio de registro de acceso de usuarios	UALSVC	Automático	Configurado		
Servicio de repositorio de estado	StateRepository	Manual	Configurado		
Servicio de sensores	SensorService	Manual	Configurado		
Servicio de servidor proxy KDC (KPS)	KPSSVC	Manual	Configurado		
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado		
Servicio de supervisión de licencias de Windows	WLMS	Automático	Configurado		
Servicio de supervisión de sensores	SensrSvc	Manual	Configurado		
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Manual	Configurado		
Servicio de uso compartido de datos	DsSvc	Manual	Configurado		
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Deshabilitado	Configurado		
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Manual	Configurado		
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual	Configurado		
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**	
Servicio de Windows Defender	WinDefend	Automático	Configurado		
Servicio de Windows Insider	wisvc	Manual	Configurado		
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado		

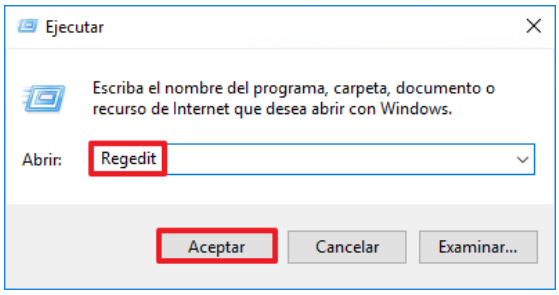
Comprobación	OK/NOK	Cómo hacerlo			
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Manual	Configurado		
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado		
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Manual	Configurado		
Servicio FrameServer de la Cámara de Windows	FrameServer	Manual	Configurado		
Servicio host de proveedor de cifrado de Windows	WEPHOSTSVC	Manual	Configurado		
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado		
Servicio Interfaz de almacenamiento en red	nsi	Automático	Configurado		
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado		
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standardcollector.service	Manual	Configurado		
Servicio telefónico	PhoneSvc	Manual	Configurado		
Servicios de cifrado	CryptSvc	Automático	Configurado		
Servicios de dominio de Active Directory	NTDS	Automático	Configurado		
Servicios de Escritorio remoto	TermService	Manual	Configurado		
Servicios web de Active Directory	ADWS	Automático	Configurado		
Servidor	LanmanServer	Automático	Configurado		
Servidor de roles de DS	DsRoleSvc	Manual	Configurado		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**	
Servidor del modelo de datos del mosaico	tiledatamodelsvc	Automático	Configurado		
Servidor DNS	DNS	Automático	Configurado		
Sincronizar host	OneSyncSvc	Automático	Configurado		
Sistema de cifrado de archivos (EFS)	EFS	Manual	Configurado		
Sistema de eventos COM+	EventSystem	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
SMP de Espacios de almacenamiento de Microsoft		smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V		vmicvss	Manual	Configurado	
Superfetch		SysMain	Manual	Configurado	
Tarjeta inteligente		SCardSvr	Deshabilitado	Configurado	
Telefonía		TapiSrv	Deshabilitado	Configurado	
Telemetría y experiencias del usuario conectado		DiagTrack	Automático	Configurado	
Temas		Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)		RpcLocator	Manual	Configurado	
WalletService		WalletService	Manual	Configurado	
Windows Driver Foundation - User-mode Driver Framework		wudfsvc	Manual	Configurado	
Windows Installer		msiserver	Manual	Configurado	
Windows Search		WSearch	Deshabilitado	Configurado	
Windows Update		wuauserv	Manual	Configurado	
21. Verifique que se han asignado los permisos correctos en el sistema de archivos		Utilizando el Explorador de Windows: **"Windows+R → Explorer"** En caso de no saber dónde apunta cada una de las rutas abreviadas que se especifica, ejecute Explorer <<ruta>> donde <<ruta>> se sustituirá por la ruta abreviada. **Nota:** Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, marcándolo con el botón derecho y eligiendo la opción "Propiedades" del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá situarse en la pestaña "Seguridad". En la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios. Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados.			

Comprobación	OK/NOK	Cómo hacerlo

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\Registration	Administrador	Control total	
	System	Control total	
	Usuario	Leer y ejecutar	
%SystemRoot%\repair	Administrador	Control total	
	System	Control total	
%SystemRoot%\security	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\cacls.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\clip.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\ras	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\rasadhlp.dll	Administrador	Control total	
%SystemRoot%\system32\rasauto.dll	Administrador	Control total	
%SystemRoot%\system32\rasautou.exe	Administrador	Control total	
%SystemRoot%\system32\raschap.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrnm.h	Administrador	Control total	
%SystemRoot%\system32\rasctrs.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrs.ini	Administrador	Control total	
%SystemRoot%\system32\rasdial.exe	Administrador	Control total	
%SystemRoot%\system32\rasmans.dll	Administrador	Control total	
%SystemRoot%\system32\rasmontr.dll	Administrador	Control total	
%SystemRoot%\system32\rasphone.exe	Administrador	Control total	
%SystemRoot%\system32\rasppp.dll	Administrador	Control total	
%SystemRoot%\system32\rastapi.dll	Administrador	Control total	
%SystemRoot%\system32\rastls.dll	Administrador	Control total	

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\system32\runonce.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\secedit.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\telnet.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tftp.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tracert.exe	Administrador	Control total	
	System	Control total	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>22. Verifique los valores del Registro.</td><td></td><td>Compruebe los valores del registro definidos en los Controladores de Dominio que pertenezcan al grupo categorizado como categoría básica siguiendo los criterios del ENS, mediante el uso del “Editor del Registro”.
“Windows+R → Regedit”
El Control de cuentas de usuario solicitará elevación de privilegios. Pulse “Sí” para continuar.
 

<table>
<tr><th>Valor del registro</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod</td><td>0</td><td></td></tr>
<tr><td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun</td><td>255</td><td></td></tr>
<tr><td>HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation</td><td>1</td><td></td></tr>
<tr><td>HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode</td><td>1</td><td></td></tr>
<tr><td>HKLM\System\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta</td><td>10</td><td></td></tr>
<tr><td>HKLM\System\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog</td><td>1</td><td></td></tr>
<tr><td>HKLM\System\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog</td><td>20000</td><td></td></tr>
</table>
</td></tr>
</table>

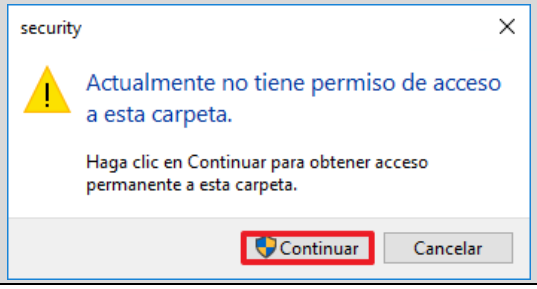
Comprobación	OK/NOK	Cómo hacerlo		
		Valor del registro	Valor	OK/NOK
		HKLM\System\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog	20	
		HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel	90	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect	0	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime	300000	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery	0	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect	1	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions	2	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions	3	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TCPMaxPortsExhausted	5	

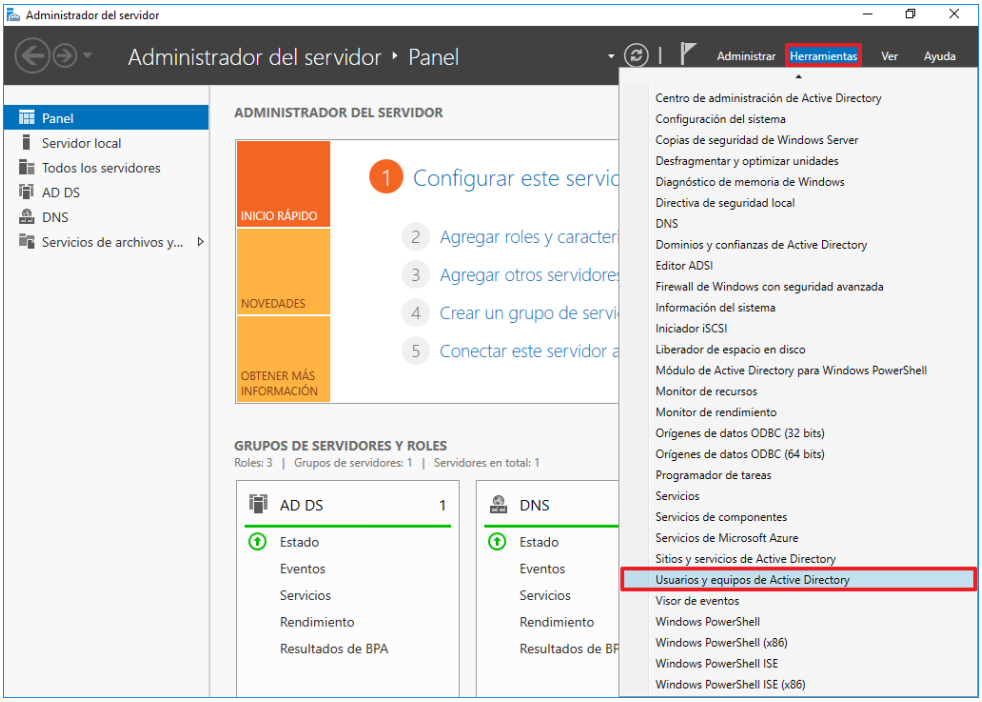
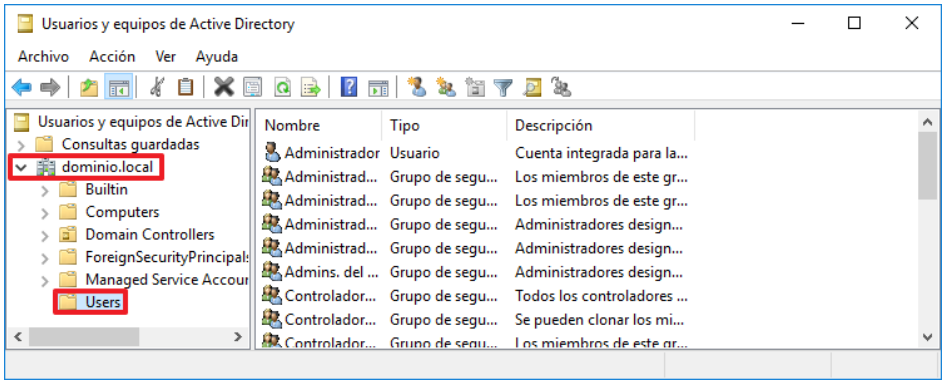
ANEXO A.2.3. GUÍA PASO A PASO SERVIDOR MIEMBRO QUE LE SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

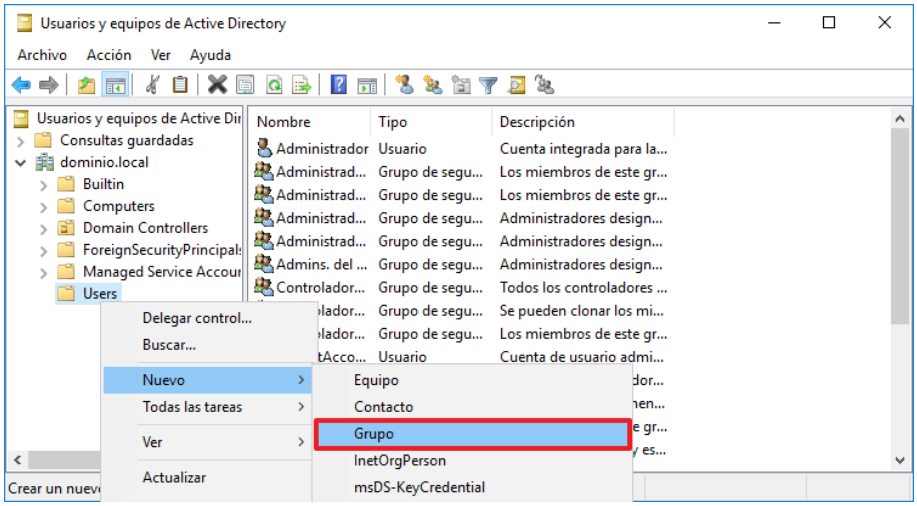
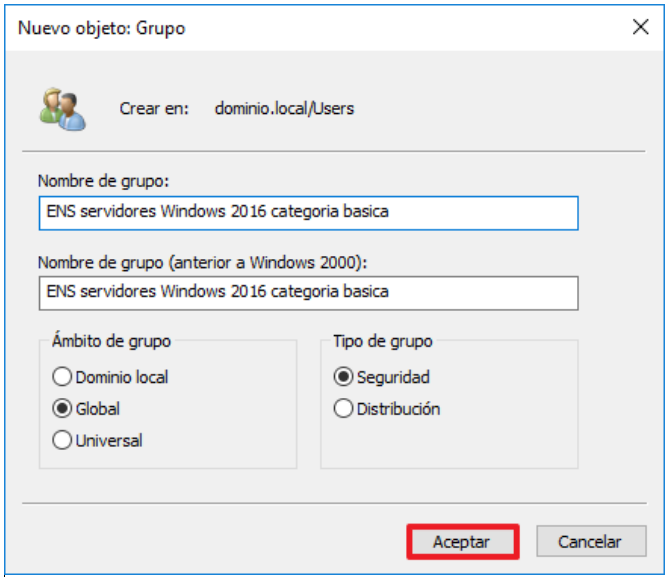
1. PREPARACIÓN DE DOMINIO

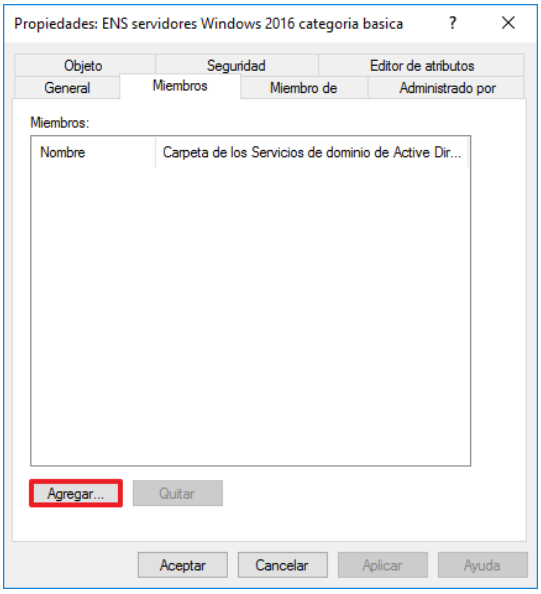
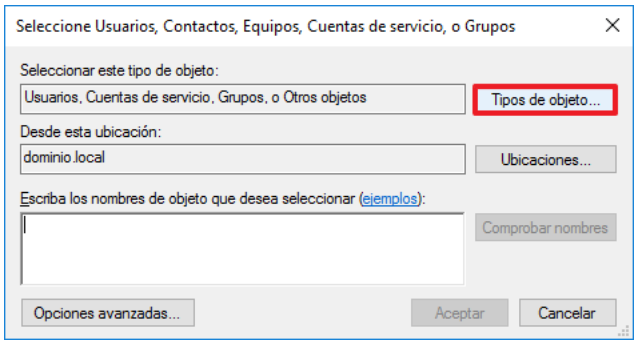
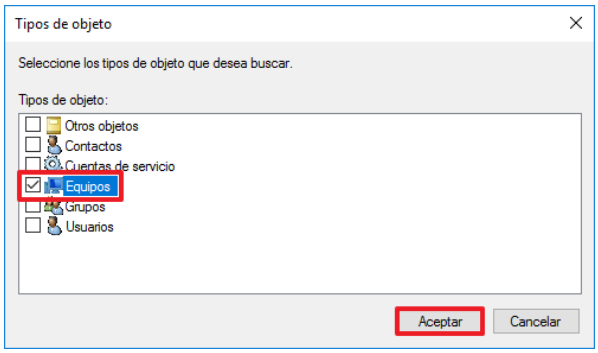
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se realizará la implementación de las plantillas de seguridad. Solo es necesario realizar este procedimiento una vez.

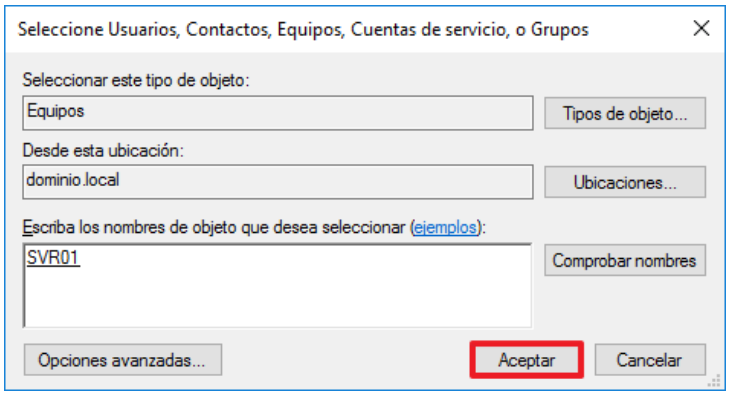
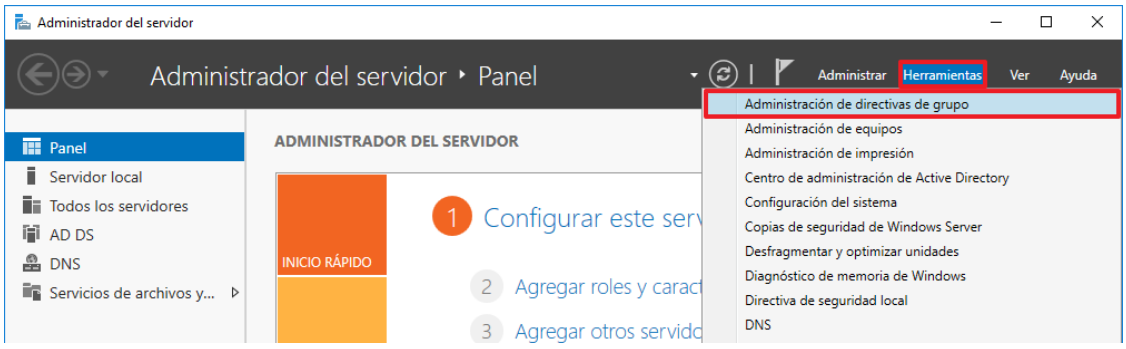
Nota: Esta guía asume que a los servidores controladores del dominio al que va a pertenecer el equipo cliente que está asegurando, se les ha aplicado la configuración descrita en el apartado "ANEXO A.2.1 GUÍA PASO A PASO CONTROLADOR DE DOMINIO QUE LE SEA DE APLICACIÓN LA CATEGORÍA BÁSICA" de la presente. Si no es así, aplique las configuraciones correspondientes al controlador de dominio, antes de continuar con la aplicación de ésta.

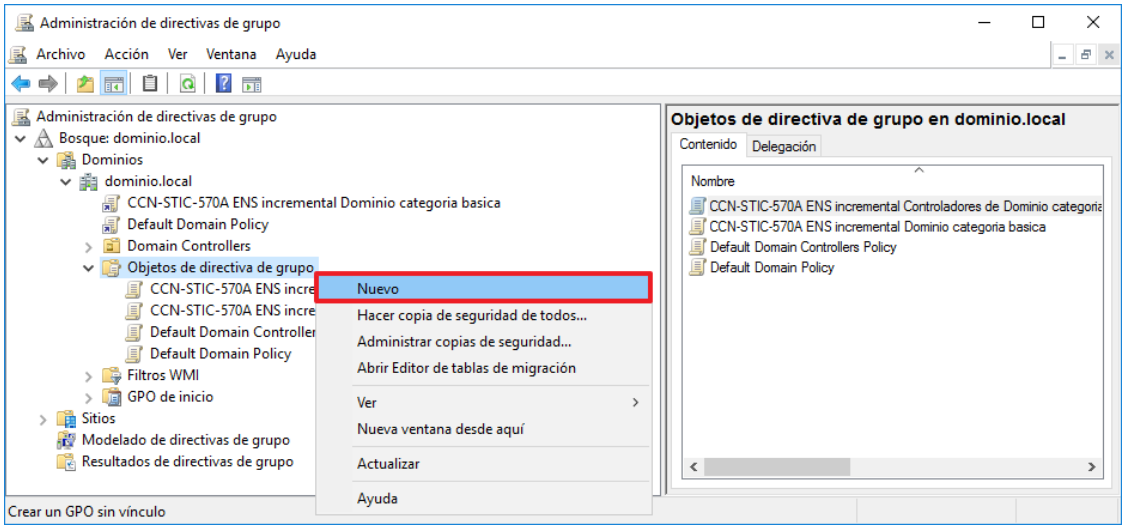
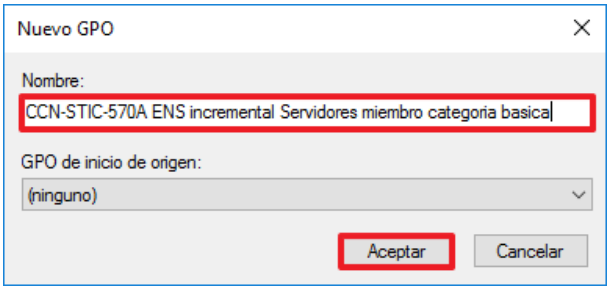
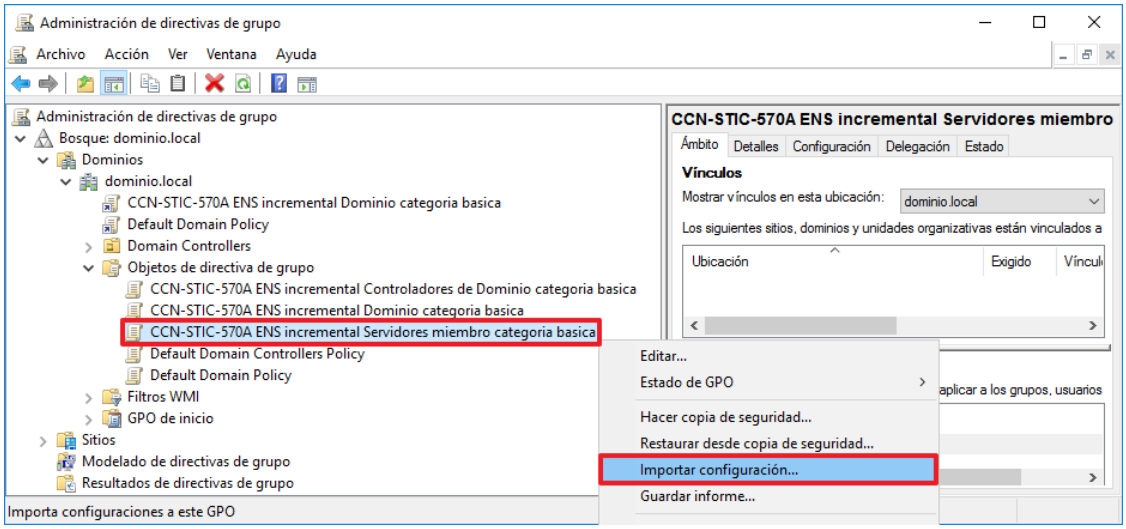
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Cree el directorio "Scripts" en la unidad C:\.
4.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts". **Nota:** Los recursos asociados a esta guía se encuentran en el directorio "Scripts-570A".
5.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio "C:\Scripts" del controlador de dominio: – CCN-STIC-570A ENS incremental DC categoria basica (directorio) – CCN-STIC-570A ENS servidores categoria basica (directorio) – CCN-STIC-570A ENS incremental DC categoria basica.inf – CCN-STIC-570A ENS incremental dominio categoria basica.inf – CCN-STIC-570A ENS Incremental servidores categoria basica.inf
6.	Copie el fichero "CCN-STIC-570A ENS incremental servidores categoria basica.inf", al directorio "%SYSTEMROOT%\Security\Templates" del Controlador de Dominio. **Nota:** Según la configuración de seguridad de UAC, el sistema podría solicitar la elevación de privilegios, en este caso, pulse "Continuar". 

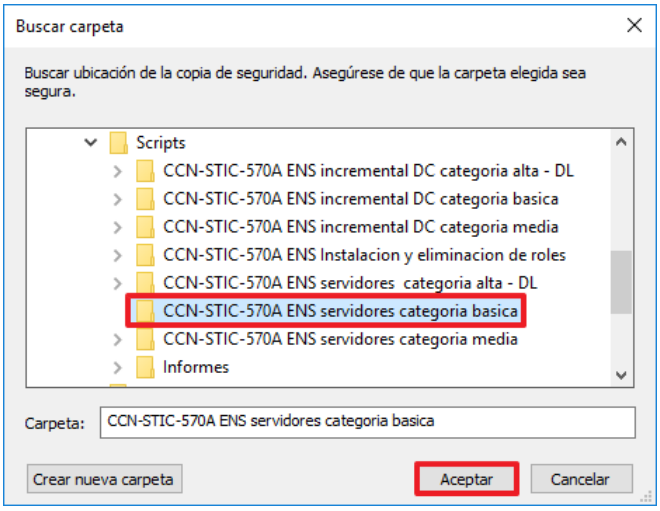
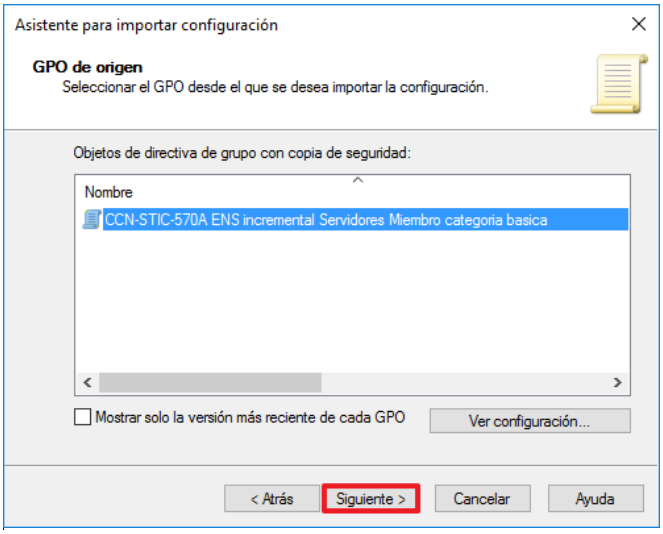
Paso	Descripción
7.	Inicie la herramienta de usuarios y equipos del Directorio Activo. Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Usuarios y equipos de Active Directory"** 
8.	Despliegue el dominio y vaya a la carpeta "Users". 

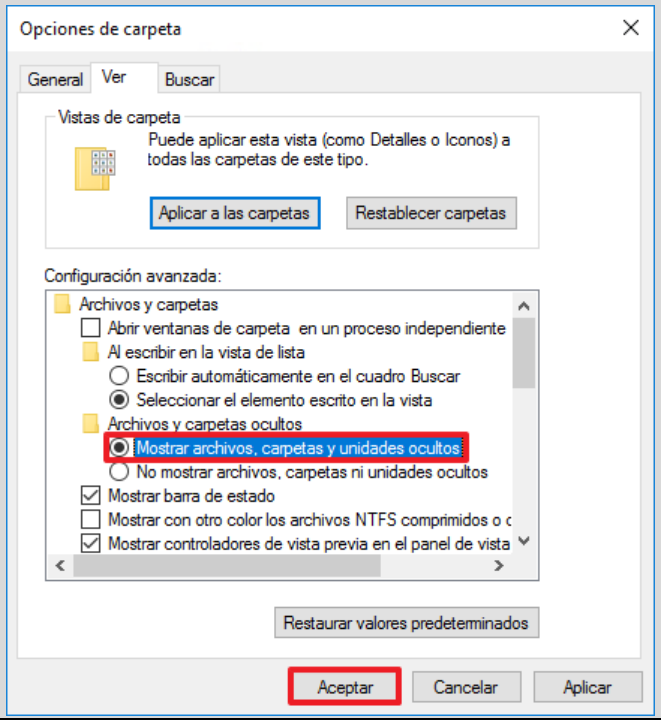
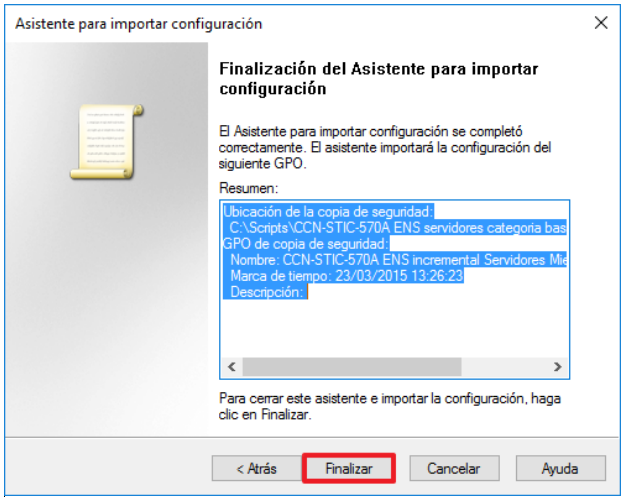
Paso	Descripción
9.	Pulse con el botón derecho sobre dicha carpeta y seleccione la opción **"Nuevo"→"Grupo".** 
10.	Introduzca como nombre "ENS servidores Windows 2016 categoria basica". Deje el resto de opciones como aparecen por defecto y pulse el botón "Aceptar". Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre servidores miembros del dominio a este grupo creado. 
11.	Abra el nuevo grupo creado pulsando doble clic sobre él y vaya a la pestaña "Miembros".

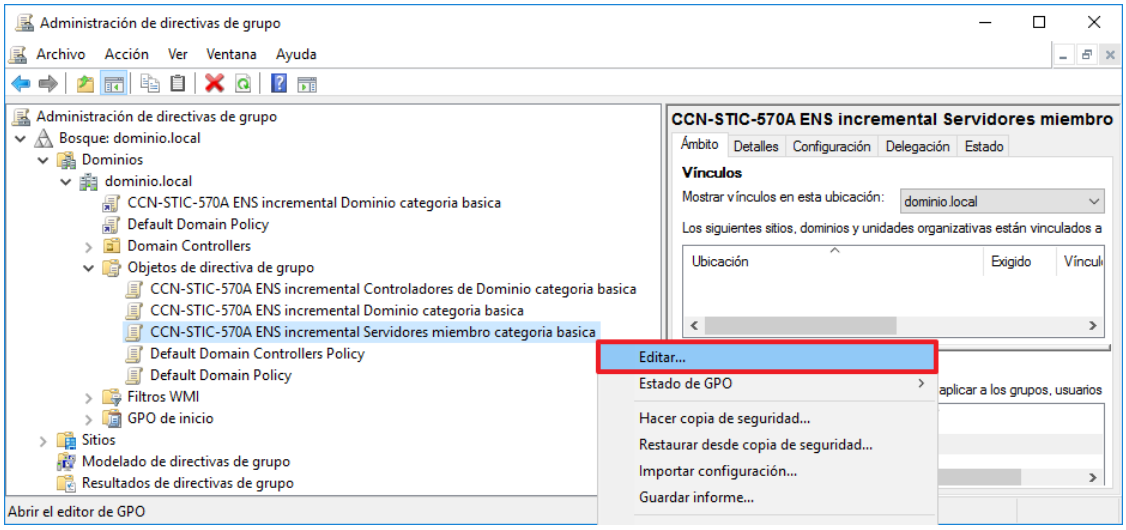
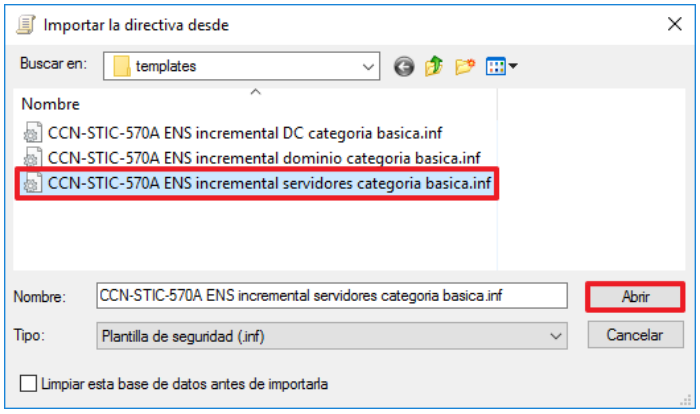
Paso	Descripción
12.	Pulse el botón “Agregar…”. 
13.	Pulse el botón “Tipos de objeto…”. 
14.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 

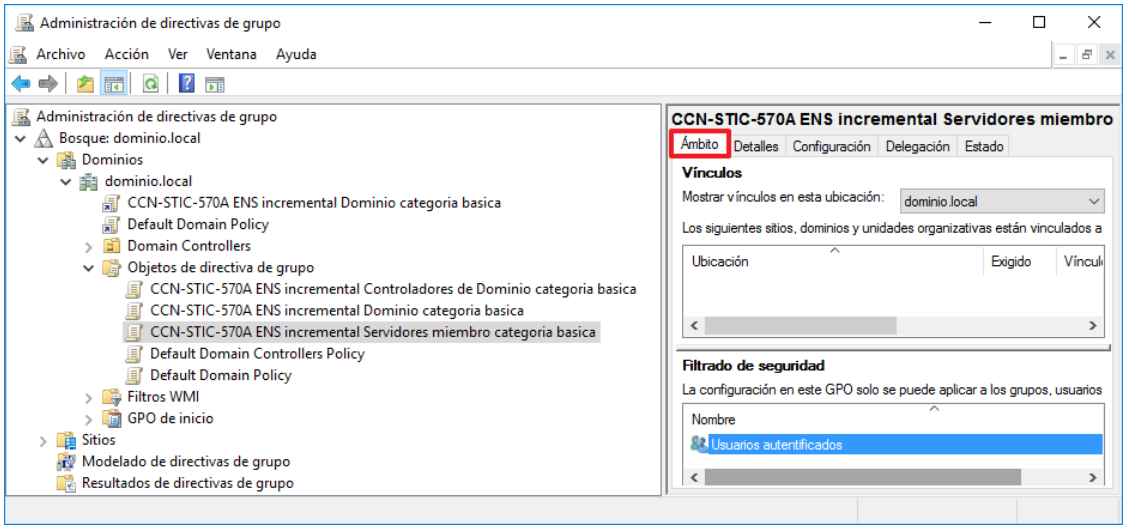
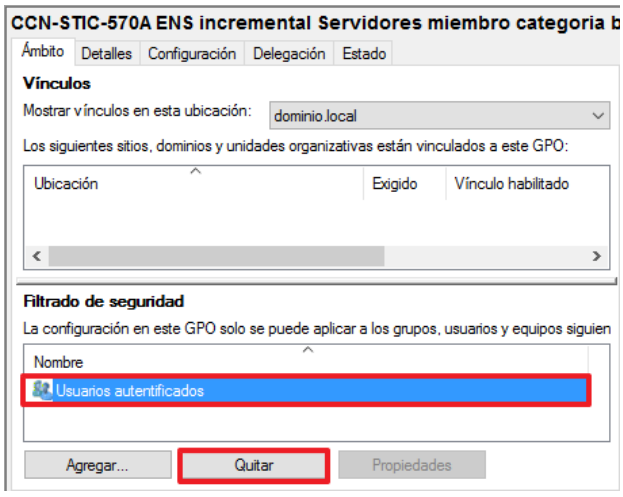
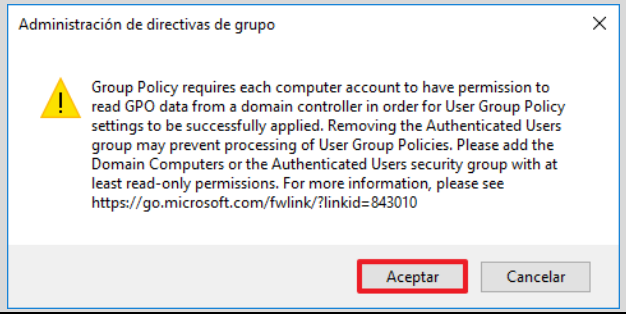
Paso	Descripción
15.	Introduzca el nombre de los servidores o utilice las opciones avanzadas para agregar todos aquellos servidores miembro que se encuentren afectados por el cumplimiento del ENS en su categoría de seguridad básica y pulse el botón “Aceptar”.  **Nota:** No agregue controladores de dominio a este grupo.
16.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo.
17.	Cierre la herramienta de “Usuarios y equipos de Directorio Activo”.
18.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”** 
19.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”.

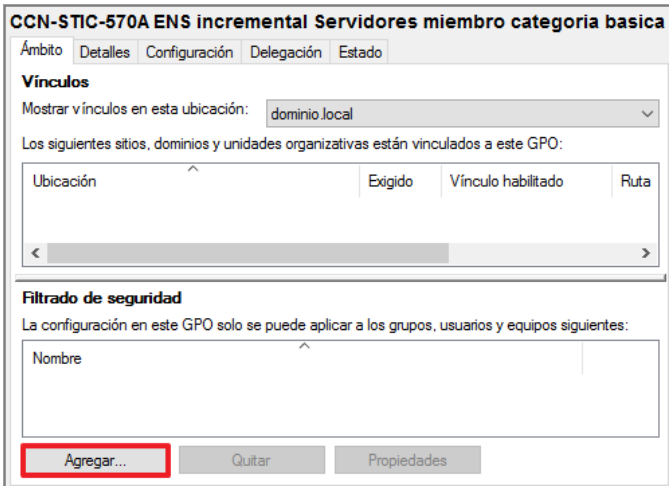
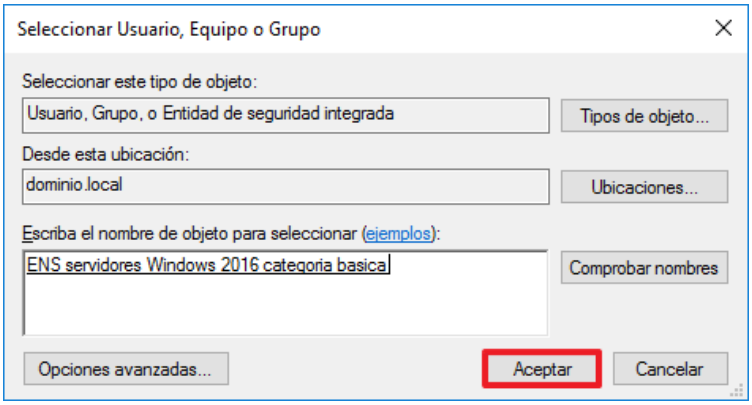
Paso	Descripción
20.	Pulse con el botón derecho, sobre dicha y carpeta y seleccione la opción “Nuevo”. 
21.	Introduzca como nombre “CCN-STIC-570A ENS incremental Servidores miembro categoria basica” y pulse el botón “Aceptar”. 
22.	La nueva política requiere una configuración de plantillas administrativas. Para ello y seleccionando la política, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración…”. 
23.	En el asistente de importación de configuración, pulse el botón “Siguiente >”.

Paso	Descripción
24.	En la selección de copia de seguridad, pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.
25.	En la “Carpeta de copia de seguridad”, pulse el botón “Examinar...”.
26.	Seleccione la carpeta “CCN-STIC-570A ENS incremental Servidores categoria basica” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 
27.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada.
28.	En la pantalla siguiente compruebe que aparece la política de seguridad de servidores de categoría básica y pulse el botón “Siguiente >”. 

Paso	Descripción
	Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero "manifest.xml". Este es un fichero oculto y, por lo tanto, debe mostrar en "opciones de carpeta", la opción "Mostrar archivos, carpetas y unidades ocultos". 
29.	En la pantalla de examen, pulse el botón "Siguiente >".
30.	Si apareciera la ventana "Migrar referencias", mantenga las opciones y pulse el botón "Siguiente >".
31.	Para completar el asistente pulse el botón "Finalizar". 
32.	Pulse el botón "Aceptar" para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración.

Paso	Descripción
33.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
34.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**
35.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva…”.
36.	Seleccione de la ruta “C:\Windows\Security\Templates” el fichero “CCN-STIC-570A ENS incremental servidores categoria basica” y pulse el botón “Abrir”. 
37.	Cierre la política de grupo.

Paso	Descripción
38.	Seleccione la nueva política de grupo configurada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 
39.	De la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
40.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. **Nota:** En caso de que aparezca la siguiente advertencia ignórela y pulse “Aceptar”. 

Paso	Descripción
41.	Una vez quitado, pulse el botón “Agregar…”. 
42.	Introduzca como nombre “ENS servidores Windows 2016 categoria basica”. Este grupo corresponde con el generado en pasos previos. A continuación, pulse el botón “Aceptar”. 
43.	Las políticas se encuentran ya creadas correctamente. No obstante, no se aplicarán hasta más adelante, una vez que haya tenido en cuenta y aplicado todas las consideraciones adicionales que se mostrarán en el siguiente punto del presente anexo. Cierre la herramienta “Administración de Directivas de Grupo”.

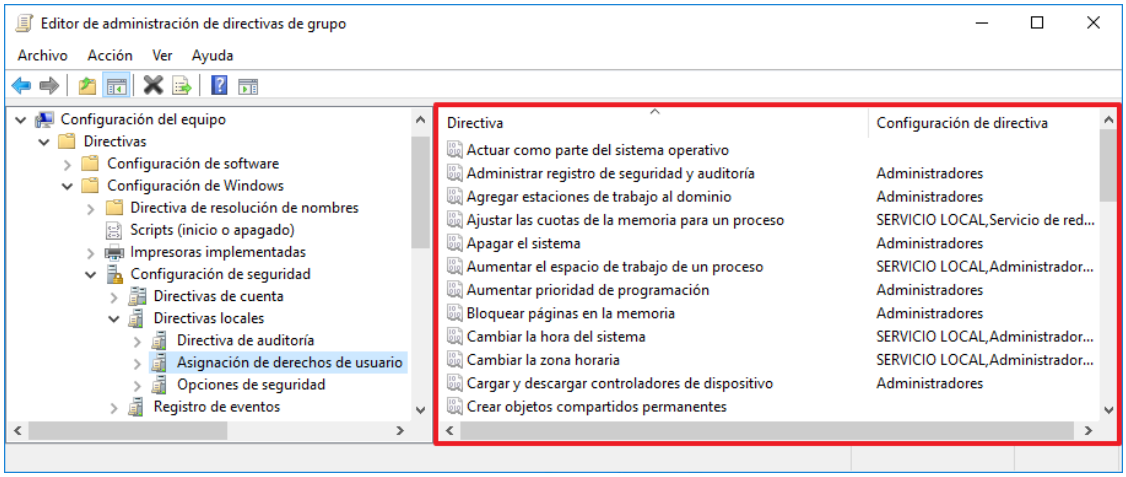
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración. Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría básica. No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

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

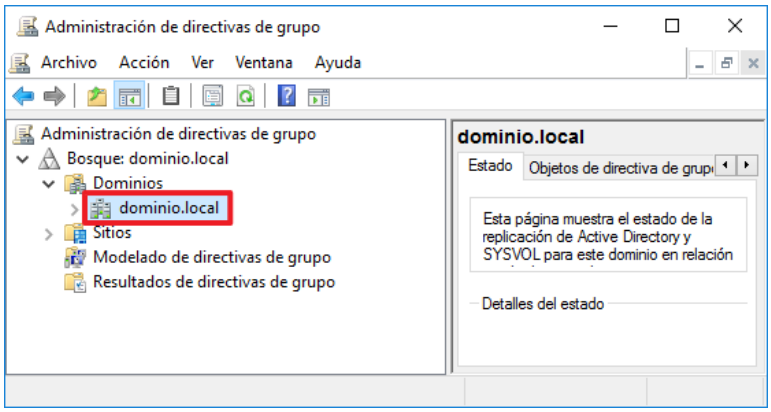
2.1. ASIGNACIÓN DE DERECHOS DE USUARIO

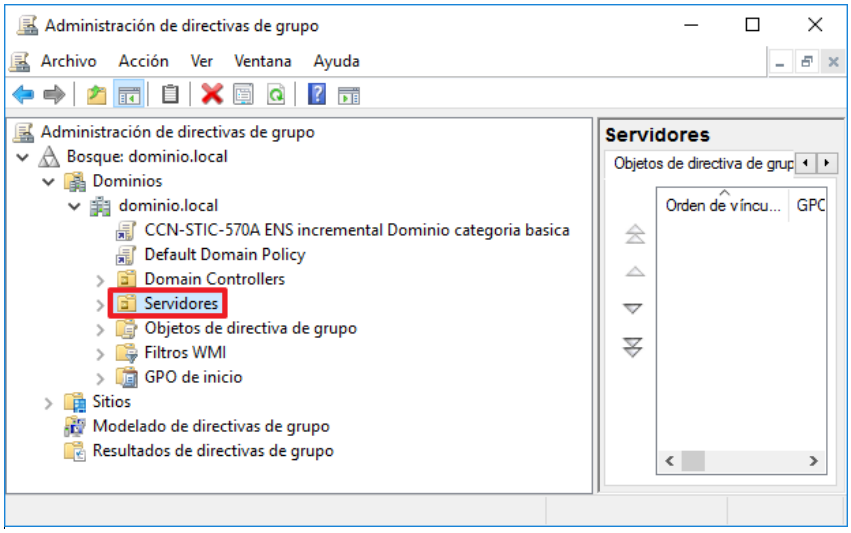
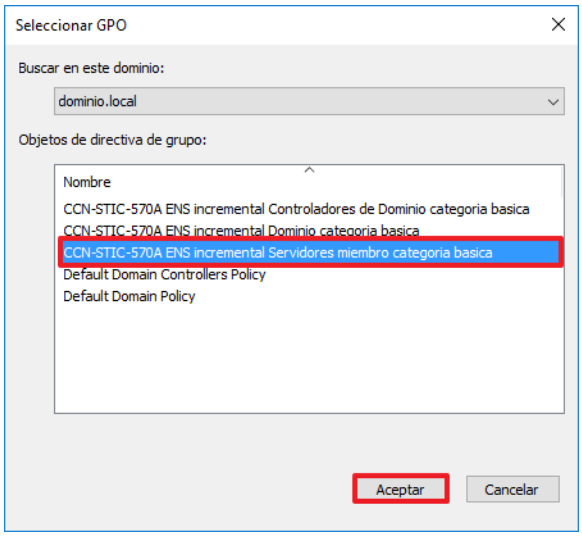
Paso	Descripción
44.	Los objetos de políticas de grupo para Controladores de Dominio y Servidores miembros especifican unos derechos de usuario siguiendo planteamientos de seguridad que aplican los principios de mínimo privilegio y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les hayan asignado derechos determinados para la administración o gestión de los sistemas. Si esto fuera así, deberá realizar las modificaciones pertinentes sobre el objeto de política de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria basica”.
45.	Edite la política de grupo correspondiente iniciando la herramienta “Administración de Directivas de Grupo” y seleccionando la política a modificar. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”** Sobre el objeto de GPO que se quiere modificar, deberá pulsar clic derecho y seleccionar “Editar” en el menú desplegado.

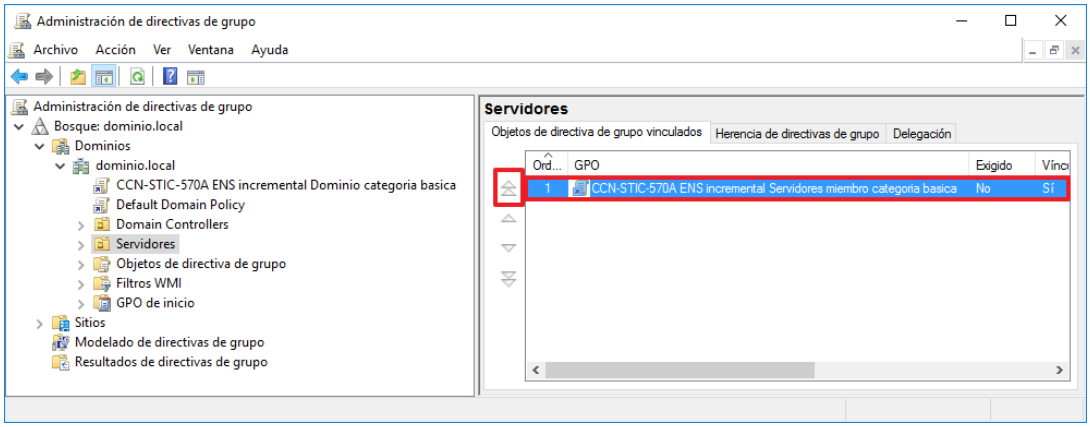
Paso	Descripción
46.	Una vez abierto el "Editor de administración de directivas de grupo", despliegue la política y sitúese en la siguiente ruta: **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"** 
47.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
48.	Guarde la configuración cerrando la ventana de editor de administración de directivas de grupo.

3. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

El presente punto establece la aplicación de las políticas de seguridad, toda vez que se han tenido en consideración las condiciones definidas en el punto previo.

Paso	Descripción
49.	Inicie la herramienta de administración de directivas de grupo.
50.	Despliegue el bloque y posiciónese sobre su dominio.  **Nota:** En el ejemplo el dominio utilizado se denomina "dominio.local".

Paso	Descripción
51.	Identifique las ubicaciones donde se encuentran los servidores Windows Server 2016 que les son de aplicación las condiciones de seguridad de categoría básica, según estipula el ENS. Sobre cada una de esas ubicaciones, asigne el objeto de política de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria basica”.  **Nota:** En el ejemplo se aplicará sobre la OU “Servidores”, que es donde se encuentran ubicados los servidores analizados en el escenario de test.
52.	Pulse con el botón derecho del ratón sobre la unidad organizativa correspondiente y selecciones la opción “Vincular un objeto GPO existente…”.
53.	Seleccione la política “CCN-STIC-570A ENS incremental Servidores miembro categoria basica” y pulse el botón “Aceptar”. 

Paso	Descripción
54.	Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-570A ENS incremental Servidores miembro categoria basica” y pulse el botón con la flecha que apunta hacia arriba hasta situarla en primer lugar dentro del orden de vínculo. 
55.	Repita los pasos 51 a 54 en cada una de las unidades organizativas donde se encuentren los servidores miembro Windows Server 2016 sujetos al cumplimiento del ENS en su categoría básica.
56.	Cierre la herramienta de administración de directivas de grupo.
57.	Elimine la carpeta “C:\Scripts”.

4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD EN LOS EQUIPOS

Las configuraciones planteadas a través de la presente guía han sido ampliamente probadas en entornos de operativa Microsoft. No obstante, no se han podido probar todas las condiciones existentes, ni con las peculiaridades de cada organización. Bajo determinadas condiciones, pudieran suceder algunas incidencias que se describen a continuación, así como su resolución.

Debe tenerse en consideración que la resolución consiste en rebajar algunos de los mecanismos de seguridad descritos en la presente guía. Por lo tanto, deberá plantearse una solución que, de forma paulatina, permita alcanzar el estado de seguridad deseado y recomendado por la presente guía.

4.1. CONTROL DE CUENTAS DE USUARIO

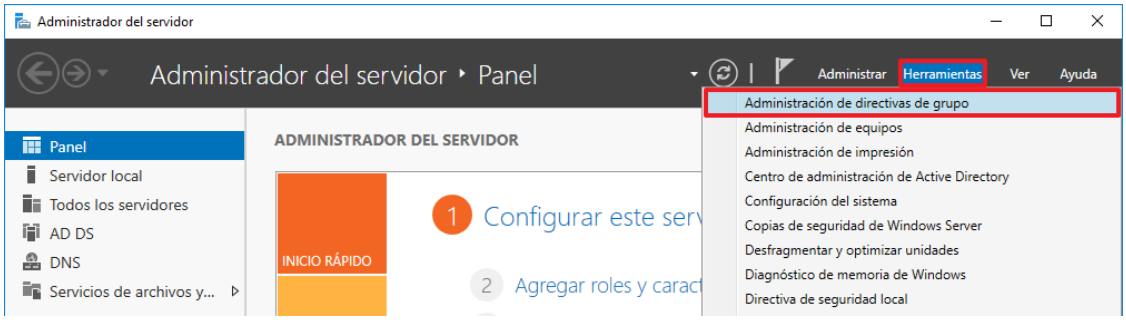
El control de cuentas de usuario surge en Windows Vista como respuesta para limitar las acciones de los administradores cuando actuaban con cuentas privilegiadas ante operativas que no requieren dicho privilegio. En sistemas previos a Windows Vista, un administrador que había iniciado una sesión actuaba siempre con los máximos privilegios, independientemente de que estuviera abriendo un fichero ofimático o estuviera navegando por internet. Puesto que el riesgo era bastante elevado, Microsoft propuso como solución UAC con objeto de advertir a los administradores cuando una acción requería privilegio para actuar.

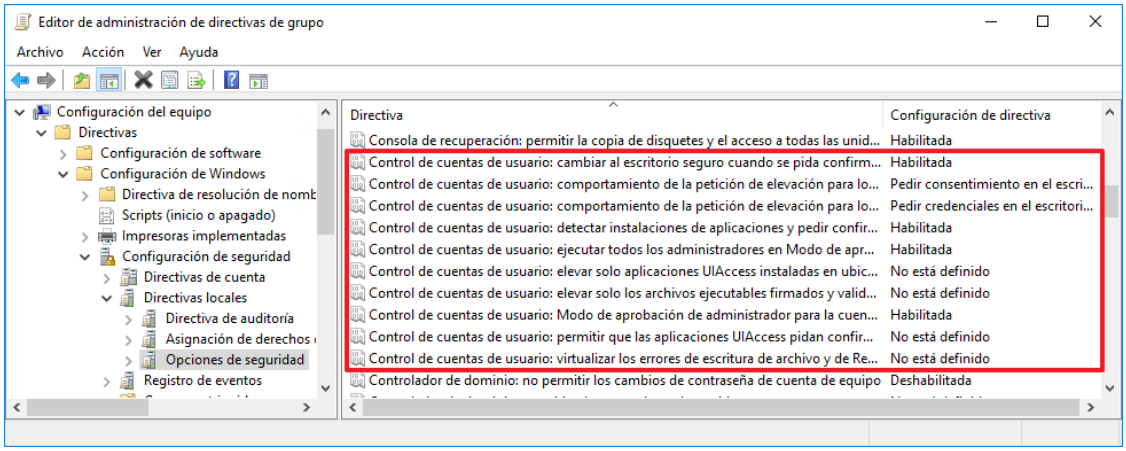
Siguiendo el principio de menor privilegio y menor exposición, la presente guía habilita las condiciones de funcionalidad de UAC para la categoría básica, aunque con los criterios más laxos de los aplicables.

No obstante, ante aplicaciones o servicios antiguos pudieran darse fallos de funcionalidad en los mismos, requiriendo que se realicen análisis o la modificación en la configuración de UAC predeterminada para la categoría básica por la presente guía.

Los siguientes pasos definen los procedimientos para la creación de una nueva política de seguridad de aplicación a los servidores que pudieran presentar incidencias con una nueva política de seguridad para el UAC.

Nota: La modificación deberá afectar exclusivamente a servidores miembro. Los controladores de dominio no deberían tener problemas en la ejecución de todos sus servicios en el modo de UAC habilitado.

Paso	Descripción
58.	Identifique los servidores que tienen problemas para la ejecución de aplicaciones y servicios y quítelos como miembros del grupo “ENS servidores Windows 2016 categoria basica”.
59.	Cree un nuevo grupo con nombre “ENS servidores miembro 2016 categoria basica incidencias UAC”, e incluya en dicho grupo los servidores miembro con una categoría básica que presenten incidencias de funcionalidad del UAC. Realice estas tareas siguiendo los pasos 7 a 17 del presente anexo.
60.	Inicie la herramienta de “Administración de directivas de grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Inicio → Herramientas Administrativas → Administración de directivas de grupo”** 
61.	Cree una nueva política de grupo con el nombre “CCN-STIC-570A ENS incremental Servidores miembro categoria basica incidencias UAC”. Siga, para ello, los pasos 18 a 37 de este anexo. A continuación vincule el objeto de política de grupo a la unidad organizativa correspondiente siguiendo los pasos 49 a 56 de este anexo.
62.	Adicionalmente, asigne la nueva política de grupo al grupo de servidores recién creado “ENS servidores miembro 2016 categoria basica incidencias UAC”. Siga, para ello, los pasos 38 a 42 de este anexo.
63.	Edite el nuevo objeto de GPO “CCN-STIC-570A ENS incremental Servidores miembro categoria basica incidencias UAC”. Para ello seleccione dicha política y seleccione la opción “Editar…”

Paso	Descripción
64.	Despliegue la política y sitúese en la siguiente ruta: **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"**
65.	Identifique las directivas relativas a "Control de cuenta de usuario". 
66.	Realice las modificaciones oportunas.
67.	Cierre la política.
68.	Para que la nueva política sea efectiva, necesita reiniciar el o los servidores. Esto es debido a que la aplicación se basa en la membresía a un grupo. La condición del miembro del grupo es adquirida por un equipo cuando inicia sesión en el dominio, cuestión que se produce cuando el equipo se reinicia. **Nota:** Debe tener en consideración que, si ha alterado la política de Control de cuentas de usuario y ésta es menos rigurosa que la propuesta en la configuración deseada por esta guía, se encuentra por debajo de los requerimientos de seguridad actuales. Debería evaluar los problemas ocasionados por las aplicaciones y servicios e intentar adaptarlos a configuraciones válidas. Es factible que si los servicios y/o aplicaciones no presentan funcionalidad con UAC presenten riesgos de seguridad notables y se esté exponiendo de forma significativa la infraestructura de la organización.

ANEXO A.2.4. LISTA DE COMPROBACIÓN DE WINDOWS SERVER 2016 SERVIDOR MIEMBRO DE DOMINIO PARA LA CATEGORÍA BÁSICA

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía "ANEXO A.2.3 GUÍA PASO A PASO SERVIDOR MIEMBRO QUE LE SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS".

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los dominios y servidores Windows Server 2016 con implementación de seguridad de categoría básica del ENS.

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

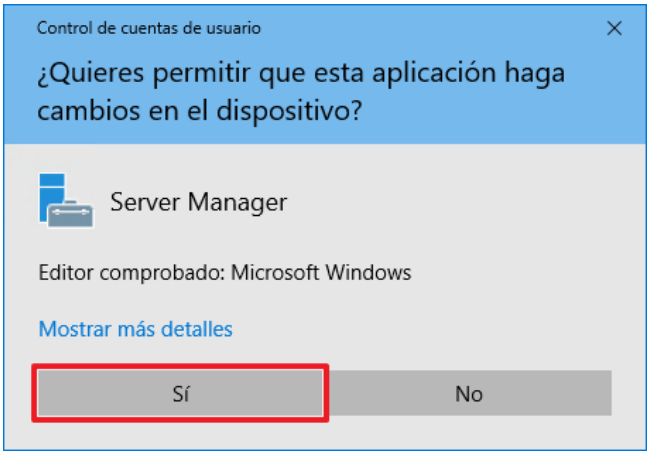
a) Administrador del Servidor.

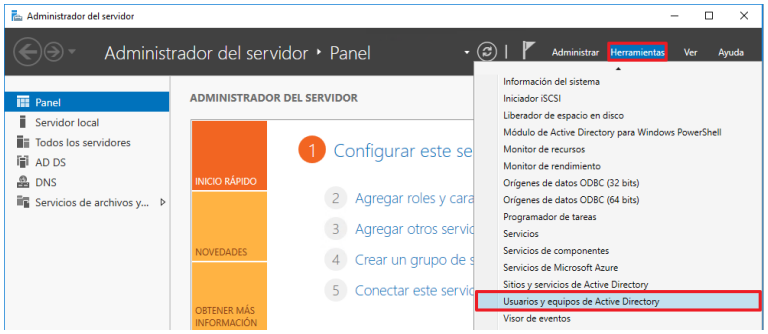
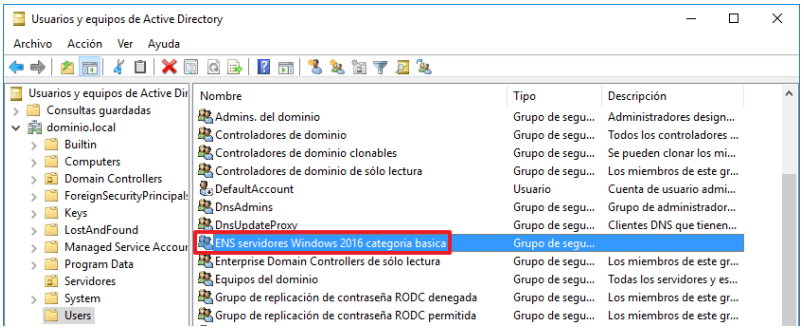
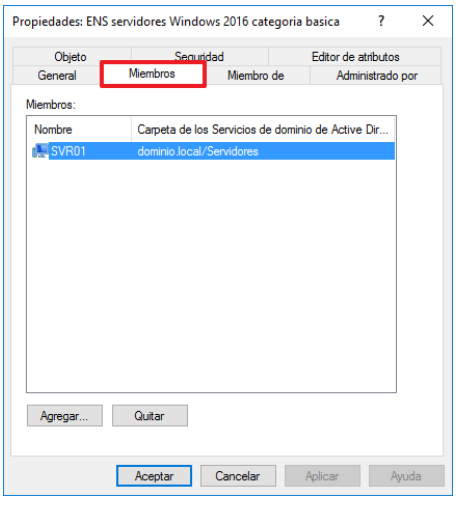
b) Conjunto resultante de directivas (rsop.msc).

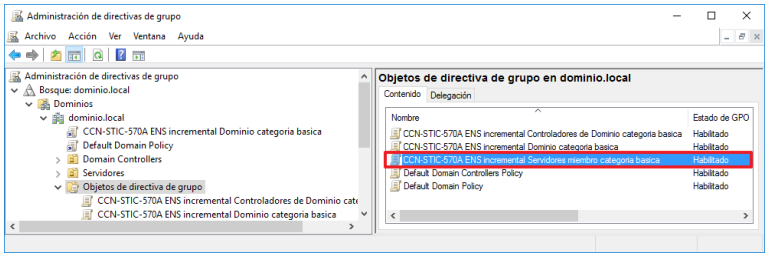
c) Consola de servicios (services.msc).

d) Editor de registro (regedit.exe).

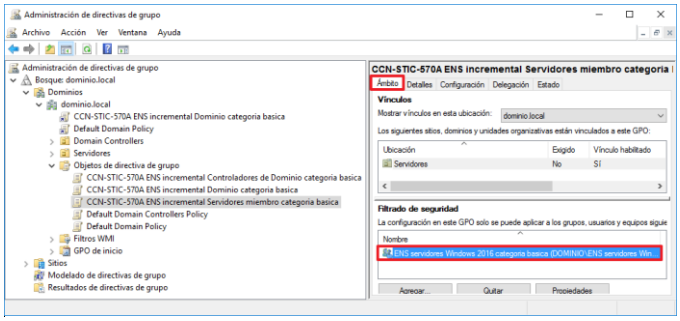
e) Explorador de Archivos (explorer.exe).

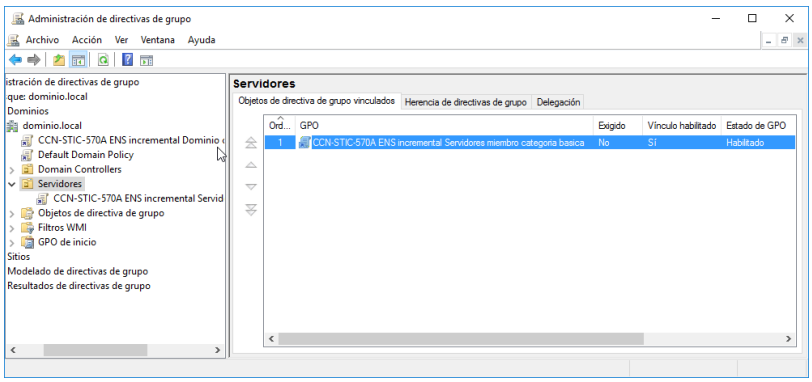
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el servidor controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Pulse "Sí" en la ventana de "Control de cuentas de usuario". 

Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que está creado el grupo “ENS servidores Windows 2016 Categoria Basica” dentro del contenedor “Users”.		Ejecute la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  Seleccione el contenedor “Users”, situado en la siguiente ruta: “**Usuarios y equipos de Active Directory → [Su dominio] → Users**” A continuación, en el panel de la derecha, verifique que está creado el objeto denominado “ENS servidores Windows 2016 categoria basica”. 
3. Verifique que los servidores que han sido catalogados como de categoría de seguridad básica y siguiendo los criterios definidos en el ENS, son miembros del grupo “ENS servidores Windows 2016 categoría Basica”.		Pulse doble clic sobre el grupo “ENS servidores Windows 2016 categoria basica” situado en el panel de la derecha y seleccione la pestaña “Miembros” para verificar que los servidores que corresponden a esta categoría de seguridad aparecen en el listado. 

Comprobación	OK/NOK	Cómo hacerlo
4. Verifique que los objetos de directivas de grupo han sido creados y están habilitados.		Ejecute la herramienta "Administrador de directivas de grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"**  Dentro de la consola diríjase a los "Objetos de directiva de grupo": **"Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo"** Verifique que está creado el objeto de directiva de grupo "CCN-STIC-570A ENS incremental Servidores miembro categoria basica" y que en la columna "Estado de GPO" figura como habilitada. 

Directiva	Valor	OK/NOK
CCN-STIC-570A ENS incremental Servidores miembro categoria basica	Habilitado	

5. Verifique que el objeto de directiva de grupo "CCN-STIC-570A ENS incremental Servidores miembro categoria basica" tiene definido el Ámbito al grupo "ENS servidores Windows 2016 categoria basica"		En el árbol de la izquierda, pulse doble clic sobre el objeto de directiva de grupo "CCN-STIC-570A ENS incremental Servidores miembro categoria basica" desde: **"Bosques [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo"** Verifique en la pestaña "Ámbito" que dentro del campo "Filtrado de seguridad" figura el grupo "ENS servidores Windows 2016 categoria basica". 

Comprobación	OK/NOK	Cómo hacerlo
6. Verifique que el objeto de directiva de grupo "CCN-STIC-570A ENS incremental Servidores miembro categoria basica" aplica a todos los objetos de las OU con servidores correspondientes a la categoría básica según los criterios del ENS y ocupa el primer lugar en el orden de vinculación.		En el árbol de la izquierda sitúese sobre las unidades organizativas con servidores correspondientes a la categoría básica según los criterios del ENS, en el ejemplo, "Servidores" desde: **"Bosque: [Su bosque] → Dominios → [Su Dominio] → Servidores"** En la pestaña "Objetos de Directiva de grupo vinculados" verifique que el objeto de directiva de grupo "CCN-STIC-570A ENS incremental Servidores miembro categoria basica" figura en el panel de la derecha y ocupa el primer lugar en la columna "Orden de Vínculos". 
7. Verifique los valores de auditoría de la directiva de grupo "CCN-STIC-570A ENS incremental servidores miembro categoria basica".		En el "Administrador de Directivas de Grupo" de uno de los controladores del dominio, pulse el botón derecho del ratón sobre la directiva desde: "**Bosque: [Su Bosque] → Dominios → [Su Dominio] → [OU de servidores] → CCN-STIC-570A ENS incremental servidores miembro categoria basica"** Seleccione la opción "Editar…". Cuando se abra el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones. Seleccione el siguiente nodo. **"Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría"**

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="11"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Auditar el acceso a objetos</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td colspan="2">Auditar el acceso del servicio de directorio</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td colspan="2">Auditar el cambio de directivas</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td colspan="2">Auditar el seguimiento de procesos</td><td>Sin auditoría</td><td></td></tr>
<tr><td colspan="2">Auditar el uso de privilegios</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td colspan="2">Auditar el acceso a objetos</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td colspan="2">Auditar eventos de inicio de sesión</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td colspan="2">Auditar eventos de inicio de sesión de cuenta</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td colspan="2">Auditar eventos del sistema</td><td>Correcto</td><td></td></tr>
<tr><td colspan="2">Auditar la administración de cuentas</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>8. Verifique los valores de asignación de derechos de usuario en la directiva de grupo “CCN-STIC-570A ENS incremental servidores miembro categoria basica”.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Administrar registro de seguridad y auditoría	Administradores	
		Agregar estaciones de trabajo al dominio	Administradores	
		Ajustar las cuotas de la memoria para un proceso	Administradores, SERVICIO LOCAL, Servicio de red	
		Apagar el sistema	Administradores	
		Aumentar el espacio de trabajo de un proceso	Administradores, SERVICIO LOCAL	
		Aumentar prioridad de programación	Administradores	
		Bloquear páginas en la memoria	Administradores	
		Cambiar la hora del sistema	SERVICIO LOCAL, Administradores	
		Cambiar la zona horaria	SERVICIO LOCAL, Administradores	
		Cargar y descargar controladores de dispositivo	Administradores	
		Crear objetos globales	Administradores, SERVICIO, SERVICIO LOCAL, Servicio de red	
		Crear un archivo de paginación	Administradores	
		Crear vínculos simbólicos	Administradores	
		Denegar el acceso desde la red a este equipo	ANONYMOUS LOGON, Invitados	
		Denegar el inicio de sesión como servicio	Invitados	
		Denegar el inicio de sesión como trabajo por lotes	Invitados	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Denegar el inicio de sesión local	Invitados	
		Denegar el inicio de sesión a través de Servicios de Escritorio Remoto	Invitados	
		Forzar cierre desde un sistema remoto	Administradores	
		Generar auditorías de seguridad	SERVICIO LOCAL, Servicio de red	
		Generar perfiles de un solo proceso	Administradores	
		Generar perfiles de rendimiento del sistema	Administradores	
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	Administradores	
		Hacer copias de seguridad de archivos y directorios	Administradores, Operadores de copia de seguridad	
		Modificar la etiqueta de un objeto	Administradores	
		Modificar valores de entorno firmware	Administradores	
		Permitir el inicio de sesión local	Administradores	
		Quitar equipo de la estación de acoplamiento	Administradores	
		Realizar tareas de mantenimiento de volumen	Administradores	
		Reemplazar un símbolo (token) de nivel de proceso	SERVICIO LOCAL, Servicio de red	
		Restaurar archivos y directorios	Administradores	
		Suplantar a un cliente tras la autenticación	Administradores, SERVICIO, SERVICIO LOCAL, Servicio de red	
		Tener acceso a este equipo desde la red	Administradores, Usuarios autentificados, ENTERPRISE DOMAIN CONTROLLERS	
		Tomar posesión de archivos y otros objetos	Administradores	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>9. Verifique los valores de las opciones de seguridad de la directiva de grupo “CCN-STIC-570A ENS incremental servidores miembro categoria basica”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de Seguridad”</td></tr>
<tr><td></td><td colspan="2">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Acceso a redes: modelo de seguridad y uso compartido para cuentas locales</td><td>Clásico: usuarios locales se autentican con credenciales propias</td><td></td></tr>
<tr><td>Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos</td><td>Deshabilitada</td><td></td></tr>
<tr><td>Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: rutas del Registro accesibles remotamente</td><td>System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, Software\Microsoft\Windows NT\CurrentVersion</td><td></td></tr>
</table>
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Acceso a redes: rutas y subrutas del Registro accesibles remotamente	Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\TerminalServer, System\CurrentControlSet\Control\TerminalServer\UserConfig, System\CurrentControlSet\Control\TerminalServer\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib, System\CurrentControlSet\Services\SysmonLog	
		Acceso de red: permitir traducción SID/nombre anónima	Deshabilitada	
		Apagado: permitir apagar el sistema sin tener que iniciar sesión	Deshabilitada	
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitada	
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada	
		Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Habilitada	
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitada	
		Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador	Pedir consentimiento en el escritorio seguro	
		Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar	Pedir credenciales en el escritorio seguro	
		Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación	Habilitada	
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitada	
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitada	
		Controlador de dominio: no permitir los cambios de contraseña de cuenta de equipo	Deshabilitada	
		Criptografía de sistema: forzar la protección con claves seguras para las claves de usuario almacenadas en el equipo	El usuario debe escribir una contraseña cada vez que use una clave.	
		Cuentas: estado de la cuenta de invitado	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitada	
		DCOM: restricciones de acceso al equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)	O:BAG:BAD: (A;;CCDCLC;;;AU)(A;;CCDCLC;;;S-1-5-32-562)	
		DCOM: restricciones de inicio al equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)	O:BAG:BAD: (A;;CCDCLCSWRP;;;BA)(A;;CCDCSW;;;AU)(A;;CCDCLCSWRP;;;S-1-5-32-562)	
		Dispositivos: permitir formatear y expulsar medios extraíbles	Administradores y usuarios avanzados	
		Dispositivos: restringir el acceso a disquetes sólo al usuario con sesión iniciada localmente	Habilitado	
		Dispositivos: restringir el acceso al CD-ROM sólo al usuario con sesión iniciada localmente	Habilitado	
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo	
		Inicio de sesión interactivo: mostrar información de usuario cuando se bloquee la sesión	No mostrar la información del usuario	
		Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr	Deshabilitada	
		Inicio de sesión interactivo: número de inicios de sesión anteriores que se almacenarán en caché (si el controlador de dominio no está disponible	1 inicios de sesión	
		Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire	14 días	
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	
		Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitada	
		Miembro de dominio: duración máxima de contraseña de cuenta de equipo	30 días	
		Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	
		Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitada	
		Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitada	
		Seguridad de red: nivel de autenticación de LAN Manager	Enviar sólo respuesta NTLMv2 y rechazar LM	
		Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada	
		Seguridad de red: permitir que LocalSystem use la identidad del equipo para NTLM	Habilitada	
		Seguridad de red: permitir retroceso a sesión NULL de LocalSystem	Deshabilitada	
		Seguridad de red: permitir solicitudes de autenticación PKU2U a este equipo para usar identidades en Internet	Deshabilitada	
		Seguridad de red: restringir NTLM: auditar el tráfico NTLM entrante	Habilitar la auditoría para todas las cuentas	
		Seguridad de red: restringir NTLM: auditar la autenticación NTLM en este dominio	Habilitar todo	
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitada	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="3"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor</td><td>Aceptar si lo proporciona el cliente</td><td></td></tr>
<tr><td colspan="2">Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión</td><td>30 minutos</td><td></td></tr>
<tr><td rowspan="12">10. Verifique el registro de eventos de la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria basica”.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro de eventos”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Evitar que el grupo de invitados locales tenga acceso al registro de aplicaciones</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Evitar que el grupo de invitados locales tenga acceso al registro de seguridad</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Evitar que el grupo de invitados locales tenga acceso al registro del sistema</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Método de retención del registro de la aplicación</td><td>Según se necesite</td><td></td></tr>
<tr><td colspan="2">Método de retención del registro de seguridad</td><td>Según se necesite</td><td></td></tr>
<tr><td colspan="2">Método de retención del registro del sistema</td><td>Según se necesite</td><td></td></tr>
<tr><td colspan="2">Tamaño máximo del registro de la aplicación</td><td>32768 kilobytes</td><td></td></tr>
<tr><td colspan="2">Tamaño máximo del registro de seguridad</td><td>163840 kilobytes</td><td></td></tr>
<tr><td colspan="2">Tamaño máximo del registro del sistema</td><td>32768 kilobytes</td><td></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
11. Verifique los servicios de sistema en la directiva de grupo "CCN-STIC-570A ENS incremental Servidores miembro categoria basica".		Seleccione el siguiente nodo. **"Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"** **Nota:** Dependiendo de los servicios que estén instalados en el equipo, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales (antivirus, etc.). En la siguiente tabla se muestran el nombre largo y el nombre corto para cada servicio. En la ventana del editor de administración de directivas de grupo sólo aparecerá uno de los dos: el nombre largo si el servicio está instalado en el sistema o el nombre corto si no lo está. Además, deberá tener en cuenta que los números existentes en algunos servicios son aleatorios y cambian en cada equipo.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado	
Administración de aplicaciones	AppMgmt	Manual	Configurado	
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado	
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado	
Administración remota de Windows (WS-Management)	WinRM	Automático	Configurado	
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado	
Administrador de conexiones de acceso remoto	RasMan	Manual	Configurado	
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado	
Administrador de credenciales	VaultSvc	Manual	Configurado	
Administrador de cuentas de seguridad	SamSs	Automático	Configurado	
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado	
Administrador de sesión local	LSM	Automático	Configurado	
Administrador de usuarios	UserManager	Automático	Configurado	
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado	
Agente de conexión de red	NcbService	Manual	Configurado	
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado	
Agente de directiva IPsec	PolicyAgent	Manual	Configurado	
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado	
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado	
Aislamiento de claves CNG	KeyIso	Manual	Configurado	
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado	
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado	
Aplicación auxiliar IP	iphlpsvc	Automático	Configurado	
Aplicación del sistema COM+	COMSysApp	Manual	Configurado	
Archivos sin conexión	CscService	Deshabilitado	Configurado	
Asignador de detección de topologías de nivel de vínculo	lltdsvc	Manual	Configurado	
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**

Comprobación	OK/NOK	Cómo hacerlo		
Asistente para la conectividad de red	NcaSvc	Manual	Configurado	
Audio de Windows	Audiosrv	Manual	Configurado	
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Deshabilitado	Configurado	
Ayudante especial de la consola de administración	sacsvr	Manual	Configurado	
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado	
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado	
CDPUserSvc	CDPUserSvc	Automático	Configurado	
Cliente de directiva de grupo	gpsvc	Automático	Configurado	
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático	Configurado	
Cliente DHCP	Dhcp	Automático	Configurado	
Cliente DNS	Dnscache	Automático	Configurado	
Cola de impresión	Spooler	Automático	Configurado	
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Manual	Configurado	
Comprobador puntual	svsvc	Manual	Configurado	
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado	
Conexiones de red	Netman	Manual	Configurado	
Configuración automática de redes cableadas	dot3svc	Manual	Configurado	
Configuración de Escritorio remoto	SessionEnv	Manual	Configurado	
Conjunto resultante de proveedor de directivas	RSoPProv	Manual	Configurado	
Contenedor de Microsoft Passport	NgcCtnrSvc	Manual	Configurado	
Coordinador de transacciones distribuidas	MSDTC	Automático	Configurado	
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
DataCollectionPublishi	DcpSvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
ngService					
Datos de contactos		PimIndexMaintenanceSvc	Manual	Configurado	
Detección de hardware shell		ShellHWDetection	Deshabilitado	Configurado	
Detección de servicios interactivos		UI0Detect	Manual	Configurado	
Detección SSDP		SSDPSRV	Deshabilitado	Configurado	
Directiva de extracción de tarjetas inteligentes		SCPolicySvc	Manual	Configurado	
Disco virtual		vds	Manual	Configurado	
Dispositivo host de UPnP		upnphost	Manual	Configurado	
DLL de host del Contador de rendimiento		PerfHost	Manual	Configurado	
dmwappushsvc		dmwappushservice	Deshabilitado	Configurado	
Energía		Power	Automático	Configurado	
Enrutamiento y acceso remoto		RemoteAccess	Deshabilitado	Configurado	
Estación de trabajo		LanmanWorkstation	Automático	Configurado	
Eventos de adquisición de imágenes estáticas		WiaRpc	Manual	Configurado	
Examinador de equipos		Browser	Deshabilitado	Configurado	
Experiencia de calidad de audio y vídeo de Windows (qWave)		QWAVE	Deshabilitado	Configurado	
Extensiones y notificaciones de impresora		PrintNotify	Manual	Configurado	
Firewall de Windows		MpsSvc	Automático	Configurado	
Hora de Windows		W32Time	Automático	Configurado	
Host de proveedor de detección de función		fdPHost	Deshabilitado	Configurado	
Host de sistema de diagnóstico		WdiSystemHost	Deshabilitado	Configurado	
Host del servicio de diagnóstico		WdiServiceHost	Deshabilitado	Configurado	
Identidad de aplicación		AppIDSvc	Manual	Configurado	
Información de la aplicación		Appinfo	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Iniciador de procesos de servidor DCOM		DcomLaunch	Automático	Configurado	
Inicio de sesión		seclogon	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
secundario					
Instalador de ActiveX (AxInstSV)		AxInstSV	Manual	Configurado	
Instalador de módulos de Windows		TrustedInstaller	Manual	Configurado	
Instantáneas de volumen		VSS	Manual	Configurado	
Instrumental de administración de Windows		Winmgmt	Automático	Configurado	
Interfaz de servicio invitado de Hyper-V		vmicguestinterface	Manual	Configurado	
KTMRM para DTC (Coordinador de transacciones distribuidas)		KtmRm	Manual	Configurado	
Llamada a procedimiento remoto (RPC)		RpcSs	Automático	Configurado	
Microsoft App-V Client		AppVClient	Deshabilitado	Configurado	
Microsoft Passport		NgcSvc	Manual	Configurado	
Modo incrustado		embeddedmode	Manual	Configurado	
Módulos de creación de claves de IPsec para IKE y AuthIP		IKEEXT	Manual	Configurado	
Motor de filtrado de base		BFE	Automático	Configurado	
Net Logon		Netlogon	Automático	Configurado	
Optimizar unidades		defragsvc	Manual	Configurado	
Partida guardada en Xbox Live		XblGameSave	Deshabilitado	Configurado	
Plug and Play		PlugPlay	Manual	Configurado	
Preparación de aplicaciones		AppReadiness	Manual	Configurado	
Programador de tareas		Schedule	Automático	Configurado	
Propagación de certificados		CertPropSvc	Manual	Configurado	
Protección de software		sppsvc	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Protocolo de autenticación extensible	Eaphost	Manual	Configurado	
Proveedor de instantáneas de software de Microsoft	swprv	Manual	Configurado	
Publicación de recurso de detección de función	FDResPub	Deshabilitado	Configurado	
Reconoc. ubicación de red	NlaSvc	Automático	Configurado	
Recopilador de eventos de Windows	Wecsvc	Manual	Configurado	
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService	Manual	Configurado	
Registro de eventos de Windows	EventLog	Automático	Configurado	
Registro remoto	RemoteRegistry	Deshabilitado	Configurado	
Registros y alertas de rendimiento	pla	Manual	Configurado	
Servicio Asistente para la compatibilidad de programas	PcaSvc	Automático	Configurado	
Servicio biométrico de Windows	WbioSrvc	Manual	Configurado	
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc	Manual	Configurado	
Servicio de administración de aplicaciones de empresa	EntAppSvc	Manual	Configurado	
Servicio de administración de radio	RmSvc	Manual	Configurado	
Servicio de administrador de licencias de Windows	LicenseManager	Manual	Configurado	
Servicio de almacenamiento	StorSvc	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**

Comprobación	OK/NOK	Cómo hacerlo			
Servicio de asociación de dispositivos		DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows		FontCache	Deshabilitado	Configurado	
Servicio de cierre de invitado de Hyper-V		vmicshutdown	Manual	Configurado	
Servicio de compatibilidad con Bluetooth		bthserv	Manual	Configurado	
Servicio de configuración de red		NetSetupSvc	Manual	Configurado	
Servicio de datos del sensor		SensorDataService	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP		WinHttpAutoProxySvc	Manual	Configurado	
Servicio de directivas de diagnóstico		DPS	Deshabilitado	Configurado	
Servicio de dispositivo de interfaz humana		hidserv	Manual	Configurado	
Servicio de enrutador de AllJoyn		AJRouter	Deshabilitado	Configurado	
Servicio de enumeración de dispositivos de tarjeta inteligente		ScDeviceEnum	Manual	Configurado	
Servicio de geolocalización		lfsvc	Manual	Configurado	
Servicio de host HV		HvHost	Manual	Configurado	
Servicio de implementación de AppX (AppXSVC)		AppXSvc	Manual	Configurado	
Servicio de infraestructura de tareas en segundo plano		BrokerInfrastructure	Automático	Configurado	
Servicio de inscripción de administración de dispositivos		DmEnrollmentSvc	Manual	Configurado	
Servicio de inspección de red de Windows Defender		WdNisSvc	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de instalación de dispositivos		DeviceInstall	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado		
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado		
Servicio de licencia de cliente (ClipSVC)	ClipSVC	Manual	Configurado		
Servicio de lista de redes	netprofm	Manual	Configurado		
Servicio de notificación de eventos de sistema	SENS	Automático	Configurado		
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService	Deshabilitado	Configurado		
Servicio de perfil de usuario	ProfSvc	Automático	Configurado		
Servicio de plataforma de dispositivos conectados	CDPSvc	Automático	Configurado		
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Manual	Configurado		
Servicio de puerta de enlace de nivel de aplicación	ALG	Manual	Configurado		
Servicio de registro de acceso de usuarios	UALSVC	Automático	Configurado		
Servicio de repositorio de estado	StateRepository	Manual	Configurado		
Servicio de sensores	SensorService	Manual	Configurado		
Servicio de servidor proxy KDC (KPS)	KPSSVC	Manual	Configurado		
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado		
Servicio de supervisión de licencias de Windows	WLMS	Automático	Configurado		
Servicio de supervisión de sensores	SensrSvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Manual	Configurado	
Servicio de uso compartido de datos	DsSvc	Manual	Configurado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Deshabilitado	Configurado	
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Manual	Configurado	
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual	Configurado	
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado	
Servicio de Windows Defender	WinDefend	Automático	Configurado	
Servicio de Windows Insider	wisvc	Manual	Configurado	
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado	
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Manual	Configurado	
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado	
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Manual	Configurado	
Servicio FrameServer de la Cámara de Windows	FrameServer	Manual	Configurado	
Servicio host de proveedor de cifrado de Windows	WEPHOSTSVC	Manual	Configurado	
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio Interfaz de	nsi	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
almacenamiento en red				
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado	
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standardcollector.service	Manual	Configurado	
Servicio telefónico	PhoneSvc	Manual	Configurado	
Servicios de cifrado	CryptSvc	Automático	Configurado	
Servicios de Escritorio remoto	TermService	Manual	Configurado	
Servidor	LanmanServer	Automático	Configurado	
Servidor del modelo de datos del mosaico	tiledatamodelsvc	Automático	Configurado	
Sincronizar host	OneSyncSvc	Automático	Configurado	
Sistema de cifrado de archivos (EFS)	EFS	Manual	Configurado	
Sistema de eventos COM+	EventSystem	Automático	Configurado	
SMP de Espacios de almacenamiento de Microsoft	smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado	
Superfetch	SysMain	Manual	Configurado	
Tarjeta inteligente	SCardSvr	Deshabilitado	Configurado	
Telefonía	TapiSrv	Deshabilitado	Configurado	
Telemetría y experiencias del usuario conectado	DiagTrack	Automático	Configurado	
Temas	Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)	RpcLocator	Manual	Configurado	
WalletService	WalletService	Manual	Configurado	
Windows Driver Foundation - User-mode Driver Framework	wudfsvc	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Windows Installer	msiserver	Manual	Configurado	
Windows Search	WSearch	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Windows Update		wuauserv	Manual	Configurado	
SMP de Espacios de almacenamiento de Microsoft		smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V		vmicvss	Manual	Configurado	
Superfetch		SysMain	Manual	Configurado	
Tarjeta inteligente		SCardSvr	Deshabilitado	Configurado	
Telefonía		TapiSrv	Deshabilitado	Configurado	
Telemetría y experiencias del usuario conectado		DiagTrack	Automático	Configurado	
Temas		Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)		RpcLocator	Manual	Configurado	
WalletService		WalletService	Manual	Configurado	
Windows Driver Foundation - User-mode Driver Framework		wudfsvc	Manual	Configurado	
Windows Installer		msiserver	Manual	Configurado	

12. Verifique los permisos de valores de registro de la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria basica”.

Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro”

Nota: Para verificar los permisos de la entrada de registro, deberá pulsar doble clic sobre la entrada **“MACHINES → SOFTWARE → Microsoft → Windows → CurrentVersion → Installer”** y pulsar sobre el botón "Modificar seguridad...".
Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".

Directiva	Valor	OK/NOK
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer	Administradores: Control Total SYSTEM: Control Total Usuarios: Leer	

Comprobación	OK/NOK	Cómo hacerlo
13. Verifique los valores del sistema de archivos de la directiva de grupo "CCN-STIC-570A ENS incremental Servidores miembro categoria basica".		Seleccione el siguiente nodo. **"Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de Archivos"** **Nota**: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción "Propiedades" del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...". Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\Registration	Administrador	Control total	
	System	Control total	
	Usuario	Leer y ejecutar	
%SystemRoot%\repair	Administrador	Control total	
	System	Control total	
%SystemRoot%\security	Administrador	Control total	
	System	Control total	
SystemRoot%\system32\cacls	Administrador	Control total	
	System	Control total	
SystemRoot%\system32\clip.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\ras	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\rasadhlp.dll	Administrador	Control total	
%SystemRoot%\system32\rasauto.dll	Administrador	Control total	
%SystemRoot%\system32\rasautou.exe	Administrador	Control total	
%SystemRoot%\system32\raschap.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrnm.h	Administrador	Control total	
%SystemRoot%\system32\rasctrs.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrs.ini	Administrador	Control total	
%SystemRoot%\system32\rasdial	Administrador	Control total	
%SystemRoot%\system32\rasmans.dll	Administrador	Control total	
%SystemRoot%\system32\rasmontr.dll	Administrador	Control total	
%SystemRoot%\system32\rasphone.exe	Administrador	Control total	
%SystemRoot%\system32\rasppp.dll	Administrador	Control total	
%SystemRoot%\system32\rastapi.dll	Administrador	Control total	
%SystemRoot%\system32\rastls.dll	Administrador	Control total	
%SystemRoot%\system32\runonce.exe	Administrador	Control total	
	System	Control total	

Comprobación	OK/NOK	Cómo hacerlo

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\system32\runonce.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\secedit.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\telnet.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tftp.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tracert.exe	Administrador	Control total	
	System	Control total	

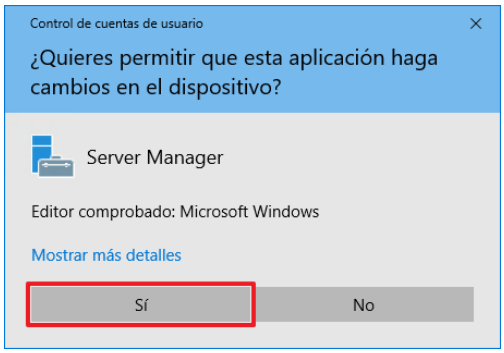
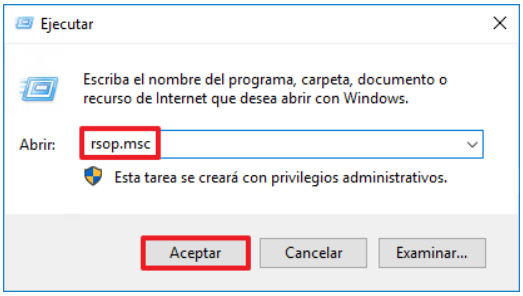
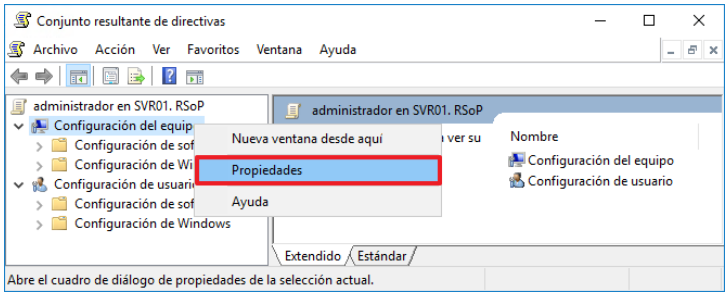
14. Verifique que está bloqueada la ejecución del Almacén digital en la directiva de grupo "CCN-STIC-570A ENS incremental Servidores miembro categoria basica".		Seleccione el siguiente nodo. **"Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Almacén Digital"**

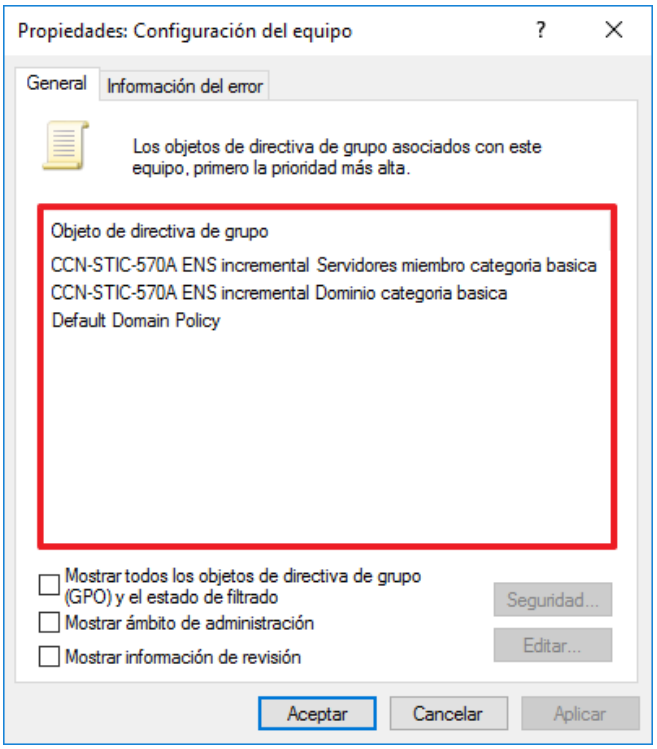
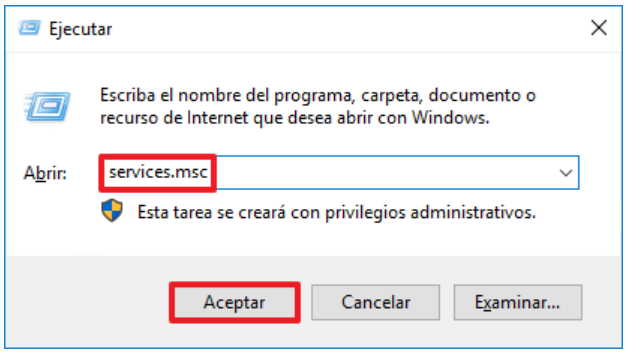
Directiva	Valor	OK/NOK
No permitir que se ejecute el Almacén digital	Habilitada	

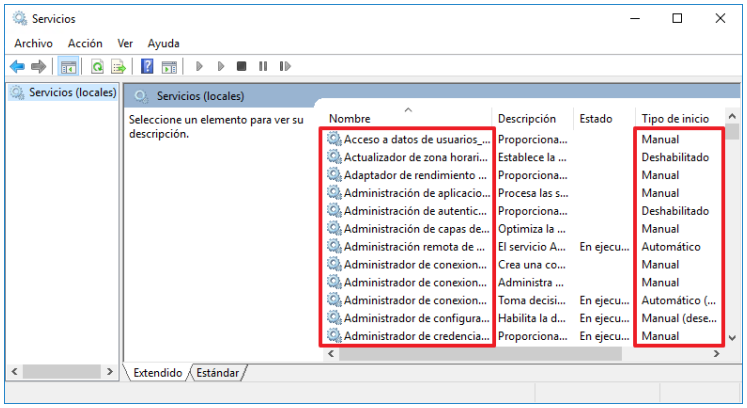
15. Verifique los valores de "Informe de errores de Windows" en la directiva de grupo "CCN-STIC-570A ENS incremental Servidores miembro categoria basica".		Seleccione el siguiente nodo. "Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Informe de errores de Windows"

Directiva	Valor	OK/NOK
Deshabilitar el informe de errores de Windows	Habilitada	
No enviar datos adicionales	Habilitada	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>16. Verifique configuración de la comunicación de Internet en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria basica”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Desactivar informe de errores de reconocimiento de escritura a mano</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el Programa para la mejora de la experiencia del usuario de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar los vínculos “Events.asp” del Visor de eventos</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el contenido “¿Sabía que…?” del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la búsqueda en Microsoft Knowledge Base del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el informe de errores de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la actualización de archivos de contenido del Asistente para búsqueda</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el acceso a la Tienda</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la tarea de imágenes “Pedir copias fotográficas”</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger</td><td>Habilitada</td><td></td></tr>
</table>
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
17. Inicie sesión en el servidor a comprobar.		Inicie sesión con una cuenta que tenga privilegios de administración del dominio en el servidor a comprobar. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Pulse "Sí" en la ventana de "Control de cuentas de usuario" 
18. Verifique que el equipo ha recibido la directiva de grupo CCN-STIC-570A ENS incremental Servidores miembro categoria basica.		Ejecute la consola de administración "Conjunto resultante de directivas" (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → rsop.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" en la ventana que se muestra a continuación:  Seleccione en ella la rama "Configuración del equipo", márquela con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la figura:  Verifique que en dicha sección aparecen listados, y por ese orden, los objetos de directiva de grupo que se indican en la siguiente tabla:

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", resaltada en la siguiente figura:
 
</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Objeto de directiva de grupo</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-570A ENS incremental Servidores miembro categoria basica</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS incremental Dominio categoria basica</td><td></td></tr>
<tr><td>Default Domain Policy</td><td></td></tr>
</table></td></tr>
<tr><td>19. Verifique que los servicios del sistema están correctamente configurados</td><td></td><td>Usando la consola de servicios (el sistema solicitará elevación de privilegios):
“Tecla Windows+R → services.msc”
El Control de cuentas de usuario solicitará elevación de privilegios. Pulse “Sí” para continuar.
 
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
		Verifique que el tipo de inicio de los servicios que aparecen en el sistema y en la siguiente tabla coinciden:  **Nota:** Dependiendo del equipo, es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales (antivirus, etc.).

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado	
Administración de aplicaciones	AppMgmt	Manual	Configurado	
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado	
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado	
Administración remota de Windows (WS-Management)	WinRM	Automático	Configurado	
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado	
Administrador de conexiones de acceso remoto	RasMan	Manual	Configurado	
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado	
Administrador de credenciales	VaultSvc	Manual	Configurado	
Administrador de cuentas de seguridad	SamSs	Automático	Configurado	
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado	
Administrador de sesión local	LSM	Automático	Configurado	
Administrador de usuarios	UserManager	Automático	Configurado	
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado	
Agente de conexión de red	NcbService	Manual	Configurado	
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado	
Agente de directiva IPsec	PolicyAgent	Manual	Configurado	
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado	
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado	
Aislamiento de claves CNG	KeyIso	Manual	Configurado	
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado	
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado	
Aplicación auxiliar IP	iphlpsvc	Automático	Configurado	
Aplicación del sistema COM+	COMSysApp	Manual	Configurado	
Archivos sin conexión	CscService	Deshabilitado	Configurado	
Asignador de detección de topologías de nivel de vínculo	lltdsvc	Manual	Configurado	
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**

Comprobación	OK/NOK	Cómo hacerlo		
Asistente para la conectividad de red	NcaSvc	Manual	Configurado	
Audio de Windows	Audiosrv	Manual	Configurado	
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Deshabilitado	Configurado	
Ayudante especial de la consola de administración	sacsvr	Manual	Configurado	
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado	
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado	
CDPUserSvc	CDPUserSvc	Automático	Configurado	
Cliente de directiva de grupo	gpsvc	Automático	Configurado	
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático	Configurado	
Cliente DHCP	Dhcp	Automático	Configurado	
Cliente DNS	Dnscache	Automático	Configurado	
Cola de impresión	Spooler	Automático	Configurado	
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Manual	Configurado	
Comprobador puntual	svsvc	Manual	Configurado	
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado	
Conexiones de red	Netman	Manual	Configurado	
Configuración automática de redes cableadas	dot3svc	Manual	Configurado	
Configuración de Escritorio remoto	SessionEnv	Manual	Configurado	
Conjunto resultante de proveedor de directivas	RSoPProv	Manual	Configurado	
Contenedor de Microsoft Passport	NgcCtnrSvc	Manual	Configurado	
Coordinador de transacciones distribuidas	MSDTC	Automático	Configurado	
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
DataCollectionPublishi	DcpSvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
ngService					
Datos de contactos		PimIndexMaintenanceSvc	Manual	Configurado	
Detección de hardware shell		ShellHWDetection	Deshabilitado	Configurado	
Detección de servicios interactivos		UI0Detect	Manual	Configurado	
Detección SSDP		SSDPSRV	Deshabilitado	Configurado	
Directiva de extracción de tarjetas inteligentes		SCPolicySvc	Manual	Configurado	
Disco virtual		vds	Manual	Configurado	
Dispositivo host de UPnP		upnphost	Manual	Configurado	
DLL de host del Contador de rendimiento		PerfHost	Manual	Configurado	
dmwappushsvc		dmwappushservice	Deshabilitado	Configurado	
Energía		Power	Automático	Configurado	
Enrutamiento y acceso remoto		RemoteAccess	Deshabilitado	Configurado	
Estación de trabajo		LanmanWorkstation	Automático	Configurado	
Eventos de adquisición de imágenes estáticas		WiaRpc	Manual	Configurado	
Examinador de equipos		Browser	Deshabilitado	Configurado	
Experiencia de calidad de audio y vídeo de Windows (qWave)		QWAVE	Deshabilitado	Configurado	
Extensiones y notificaciones de impresora		PrintNotify	Manual	Configurado	
Firewall de Windows		MpsSvc	Automático	Configurado	
Hora de Windows		W32Time	Automático	Configurado	
Host de proveedor de detección de función		fdPHost	Deshabilitado	Configurado	
Host de sistema de diagnóstico		WdiSystemHost	Deshabilitado	Configurado	
Host del servicio de diagnóstico		WdiServiceHost	Deshabilitado	Configurado	
Identidad de aplicación		AppIDSvc	Manual	Configurado	
Información de la aplicación		Appinfo	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Iniciador de procesos de servidor DCOM		DcomLaunch	Automático	Configurado	
Inicio de sesión		seclogon	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
secundario					
Instalador de ActiveX (AxInstSV)		AxInstSV	Manual	Configurado	
Instalador de módulos de Windows		TrustedInstaller	Manual	Configurado	
Instantáneas de volumen		VSS	Manual	Configurado	
Instrumental de administración de Windows		Winmgmt	Automático	Configurado	
Interfaz de servicio invitado de Hyper-V		vmicguestinterface	Manual	Configurado	
KTMRM para DTC (Coordinador de transacciones distribuidas)		KtmRm	Manual	Configurado	
Llamada a procedimiento remoto (RPC)		RpcSs	Automático	Configurado	
Microsoft App-V Client		AppVClient	Deshabilitado	Configurado	
Microsoft Passport		NgcSvc	Manual	Configurado	
Modo incrustado		embeddedmode	Manual	Configurado	
Módulos de creación de claves de IPsec para IKE y AuthIP		IKEEXT	Manual	Configurado	
Motor de filtrado de base		BFE	Automático	Configurado	
Net Logon		Netlogon	Automático	Configurado	
Optimizar unidades		defragsvc	Manual	Configurado	
Partida guardada en Xbox Live		XblGameSave	Deshabilitado	Configurado	
Plug and Play		PlugPlay	Manual	Configurado	
Preparación de aplicaciones		AppReadiness	Manual	Configurado	
Programador de tareas		Schedule	Automático	Configurado	
Propagación de certificados		CertPropSvc	Manual	Configurado	
Protección de software		sppsvc	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Protocolo de autenticación extensible	Eaphost	Manual	Configurado	
Proveedor de instantáneas de software de Microsoft	swprv	Manual	Configurado	
Publicación de recurso de detección de función	FDResPub	Deshabilitado	Configurado	
Reconoc. ubicación de red	NlaSvc	Automático	Configurado	
Recopilador de eventos de Windows	Wecsvc	Manual	Configurado	
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService	Manual	Configurado	
Registro de eventos de Windows	EventLog	Automático	Configurado	
Registro remoto	RemoteRegistry	Deshabilitado	Configurado	
Registros y alertas de rendimiento	pla	Manual	Configurado	
Servicio Asistente para la compatibilidad de programas	PcaSvc	Automático	Configurado	
Servicio biométrico de Windows	WbioSrvc	Manual	Configurado	
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc	Manual	Configurado	
Servicio de administración de aplicaciones de empresa	EntAppSvc	Manual	Configurado	
Servicio de administración de radio	RmSvc	Manual	Configurado	
Servicio de administrador de licencias de Windows	LicenseManager	Manual	Configurado	
Servicio de almacenamiento	StorSvc	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**

Comprobación	OK/NOK	Cómo hacerlo			
Servicio de asociación de dispositivos		DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows		FontCache	Deshabilitado	Configurado	
Servicio de cierre de invitado de Hyper-V		vmicshutdown	Manual	Configurado	
Servicio de compatibilidad con Bluetooth		bthserv	Manual	Configurado	
Servicio de configuración de red		NetSetupSvc	Manual	Configurado	
Servicio de datos del sensor		SensorDataService	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP		WinHttpAutoProxySvc	Manual	Configurado	
Servicio de directivas de diagnóstico		DPS	Deshabilitado	Configurado	
Servicio de dispositivo de interfaz humana		hidserv	Manual	Configurado	
Servicio de enrutador de AllJoyn		AJRouter	Deshabilitado	Configurado	
Servicio de enumeración de dispositivos de tarjeta inteligente		ScDeviceEnum	Manual	Configurado	
Servicio de geolocalización		lfsvc	Manual	Configurado	
Servicio de host HV		HvHost	Manual	Configurado	
Servicio de implementación de AppX (AppXSVC)		AppXSvc	Manual	Configurado	
Servicio de infraestructura de tareas en segundo plano		BrokerInfrastructure	Automático	Configurado	
Servicio de inscripción de administración de dispositivos		DmEnrollmentSvc	Manual	Configurado	
Servicio de inspección de red de Windows Defender		WdNisSvc	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de instalación de dispositivos		DeviceInstall	Manual	Configurado	

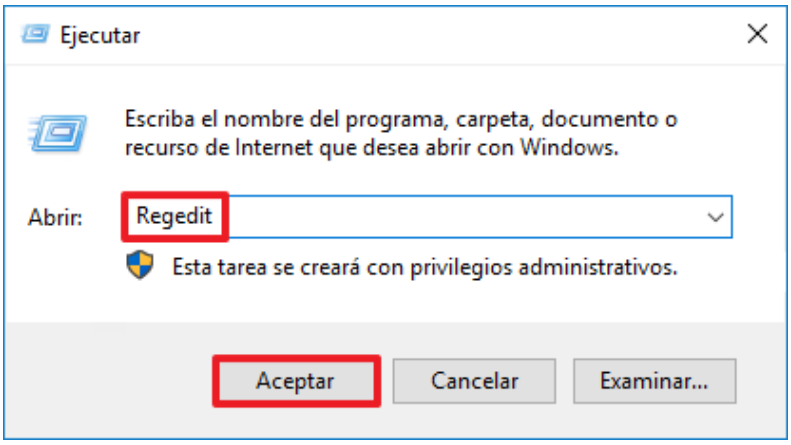
Comprobación	OK/NOK	Cómo hacerlo			
Servicio de intercambio de datos de Hyper-V		vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V		vmicheartbeat	Manual	Configurado	
Servicio de licencia de cliente (ClipSVC)		ClipSVC	Manual	Configurado	
Servicio de lista de redes		netprofm	Manual	Configurado	
Servicio de notificación de eventos de sistema		SENS	Automático	Configurado	
Servicio de Panel de escritura a mano y teclado táctil		TabletInputService	Deshabilitado	Configurado	
Servicio de perfil de usuario		ProfSvc	Automático	Configurado	
Servicio de plataforma de dispositivos conectados		CDPSvc	Automático	Configurado	
Servicio de protocolo de túnel de sockets seguros		SstpSvc	Manual	Configurado	
Servicio de puerta de enlace de nivel de aplicación		ALG	Manual	Configurado	
Servicio de registro de acceso de usuarios		UALSVC	Automático	Configurado	
Servicio de repositorio de estado		StateRepository	Manual	Configurado	
Servicio de sensores		SensorService	Manual	Configurado	
Servicio de servidor proxy KDC (KPS)		KPSSVC	Manual	Configurado	
Servicio de sincronización de hora de Hyper-V		vmictimesync	Manual	Configurado	
Servicio de supervisión de licencias de Windows		WLMS	Automático	Configurado	
Servicio de supervisión de sensores		SensrSvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Manual	Configurado	
Servicio de uso compartido de datos	DsSvc	Manual	Configurado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Deshabilitado	Configurado	
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Manual	Configurado	
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual	Configurado	
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado	
Servicio de Windows Defender	WinDefend	Automático	Configurado	
Servicio de Windows Insider	wisvc	Manual	Configurado	
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado	
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Manual	Configurado	
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado	
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Manual	Configurado	
Servicio FrameServer de la Cámara de Windows	FrameServer	Manual	Configurado	
Servicio host de proveedor de cifrado de Windows	WEPHOSTSVC	Manual	Configurado	
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio Interfaz de	nsi	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
almacenamiento en red					
Servicio PowerShell Direct de Hyper-V		vmicvmsession	Manual	Configurado	
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)		diagnosticshub.standardcollector.service	Manual	Configurado	
Servicio telefónico		PhoneSvc	Manual	Configurado	
Servicios de cifrado		CryptSvc	Automático	Configurado	
Servicios de Escritorio remoto		TermService	Manual	Configurado	
Servidor		LanmanServer	Automático	Configurado	
Servidor del modelo de datos del mosaico		tiledatamodelsvc	Automático	Configurado	
Sincronizar host		OneSyncSvc	Automático	Configurado	
Sistema de cifrado de archivos (EFS)		EFS	Manual	Configurado	
Sistema de eventos COM+		EventSystem	Automático	Configurado	
SMP de Espacios de almacenamiento de Microsoft		smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V		vmicvss	Manual	Configurado	
Superfetch		SysMain	Manual	Configurado	
Tarjeta inteligente		SCardSvr	Deshabilitado	Configurado	
Telefonía		TapiSrv	Deshabilitado	Configurado	
Telemetría y experiencias del usuario conectado		DiagTrack	Automático	Configurado	
Temas		Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)		RpcLocator	Manual	Configurado	
WalletService		WalletService	Manual	Configurado	
Windows Driver Foundation - User-mode Driver Framework		wudfsvc	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Windows Installer		msiserver	Manual	Configurado	
Windows Search		WSearch	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Windows Update		wuauserv	Manual	Configurado	
SMP de Espacios de almacenamiento de Microsoft		smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V		vmicvss	Manual	Configurado	
Superfetch		SysMain	Manual	Configurado	
Tarjeta inteligente		SCardSvr	Deshabilitado	Configurado	
Telefonía		TapiSrv	Deshabilitado	Configurado	
Telemetría y experiencias del usuario conectado		DiagTrack	Automático	Configurado	
Temas		Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)		RpcLocator	Manual	Configurado	
WalletService		WalletService	Manual	Configurado	
Windows Driver Foundation - User-mode Driver Framework		wudfsvc	Manual	Configurado	
Windows Installer		msiserver	Manual	Configurado	
20. Verifique que se han asignado los permisos correctos en el sistema de archivos		Utilizando el Explorador de Windows: **"Windows+R → Explorer"** En caso de no saber dónde apunta cada una de las rutas abreviadas que se especifica, ejecute Explorer <<ruta>> donde <<ruta>> se sustituirá por la ruta abreviada. **Nota:** Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, marcándolo con el botón derecho y eligiendo la opción "Propiedades" del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá situarse en la pestaña "Seguridad". En la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios. Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados.			

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		**Usuario**	**Permiso**	**OK/NOK**
%SystemRoot%\Registration		Administrador	Control total	
		System	Control total	
		Usuario	Leer y ejecutar	
%SystemRoot%\repair		Administrador	Control total	
		System	Control total	
%SystemRoot%\security		Administrador	Control total	
		System	Control total	
SystemRoot%\system32\cacls.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\clip.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\ras		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\rasadhlp.dll		Administrador	Control total	
%SystemRoot%\system32\rasauto.dll		Administrador	Control total	
%SystemRoot%\system32\rasautou.exe		Administrador	Control total	
%SystemRoot%\system32\raschap.dll		Administrador	Control total	
%SystemRoot%\system32\rasctrnm.h		Administrador	Control total	
%SystemRoot%\system32\rasctrs.dll		Administrador	Control total	
%SystemRoot%\system32\rasctrs.ini		Administrador	Control total	
%SystemRoot%\system32\rasdial.exe		Administrador	Control total	
%SystemRoot%\system32\rasmans.dll		Administrador	Control total	
%SystemRoot%\system32\rasmontr.dll		Administrador	Control total	
%SystemRoot%\system32\rasphone.exe		Administrador	Control total	
%SystemRoot%\system32\rasppp.dll		Administrador	Control total	
%SystemRoot%\system32\rastapi.dll		Administrador	Control total	
%SystemRoot%\system32\rastls.dll		Administrador	Control total	
%SystemRoot%\system32\runonce.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\secedit.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\telnet.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\tftp.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\tracert.exe		Administrador	Control total	
		System	Control total	

Comprobación	OK/NOK	Cómo hacerlo
21. Verifique los valores del registro.		Compruebe los valores del registro definidos en los Controladores de Dominio que pertenezcan al grupo categorizado como categoría básica siguiendo los criterios del ENS, mediante el uso del "Editor del Registro". **"Windows+R → Regedit"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" para continuar. 

Valor del registro	Valor	OK/NOK
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod	0	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun	255	
HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation	1	
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode	1	
HKLM\System\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta	10	
HKLM\System\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog	1	
HKLM\System\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog	20000	
HKLM\System\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog	20	
HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel	90	
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect	0	
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime	300000	

Comprobación	OK/NOK	Cómo hacerlo		
		Valor del registro	Valor	OK/NOK
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery	0	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect	1	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions	2	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions	3	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TCPMaxPortsExhausted	5	

ANEXO A.3. CATEGORÍA MEDIA

ANEXO A.3.1. GUÍA PASO A PASO CONTROLADOR DE DOMINIO QUE LE SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se emplee Windows Server 2016, con una categorización de seguridad media y según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este anexo, la organización deberá haber realizado la categorización de los sistemas, con objeto de determinar la categoría de cada una de las dimensiones de seguridad y según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para los servicios e información manejados por la organización correspondieran, al menos, a la categoría media para alguno de ellos y ninguno a la categoría alta, se deberán realizar las implementaciones según se referencian en el presente anexo.

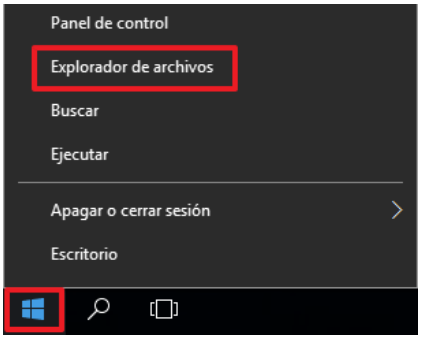
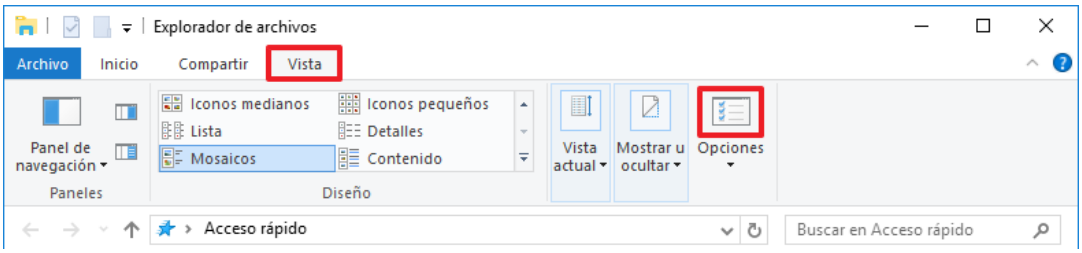
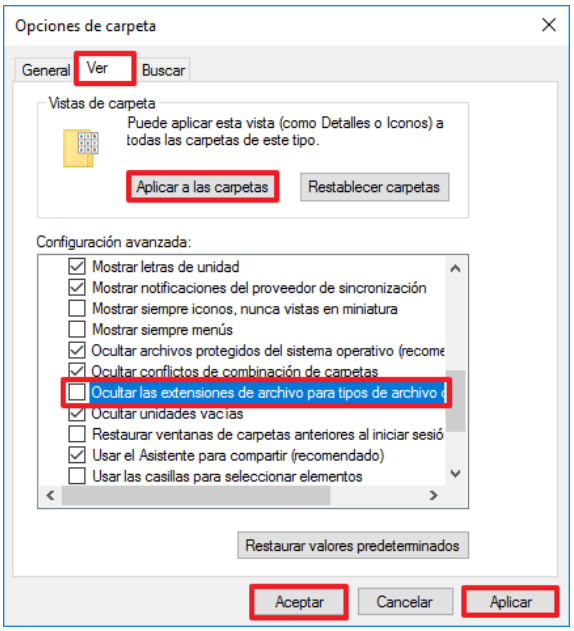
Se debe tener en cuenta que la política global definirá, a través del análisis de cada una de sus dimensiones de seguridad, el nivel de la organización. No obstante, pudiera ser factible que alguno de los servidores proporcionara servicios o gestionara información sujeta a la categoría básica. Por lo tanto, a estos servidores les podrían ser de aplicación las plantillas de seguridad correspondientes a la categoría básica establecidas en el ANEXO A.2 de la presente guía. Se deben seguir, para ellos, los pasos establecidos para la generación y aplicación de objetos de políticas de grupo para servidores miembros definidos en los puntos 1 y 3 del anexo previo. Sin embargo, las políticas de dominio y controladores de dominio, al ser de ámbito general, deberán especificar las correspondientes a esta categoría media siguiendo las pautas establecidas en los pasos posteriores.

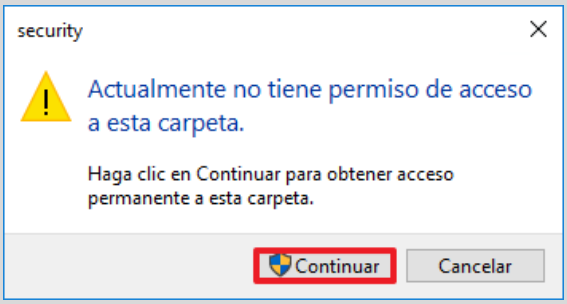
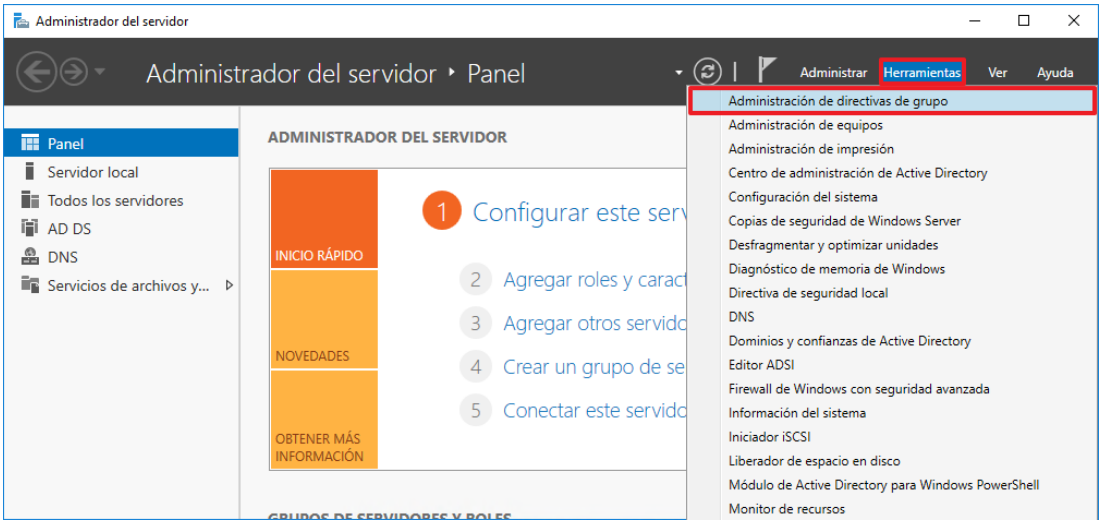
Se debe tener en consideración que, antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, se deberán realizar pruebas en un entorno de preproducción con el objeto de familiarizarse con el escenario y realizar las pruebas de funcionalidad oportunas.

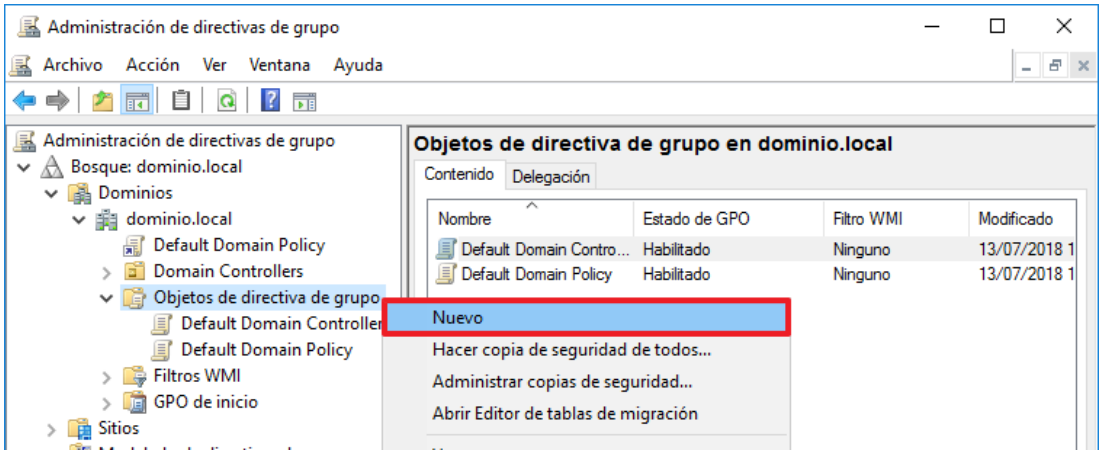
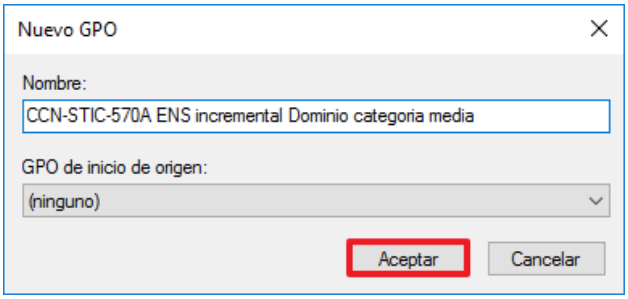
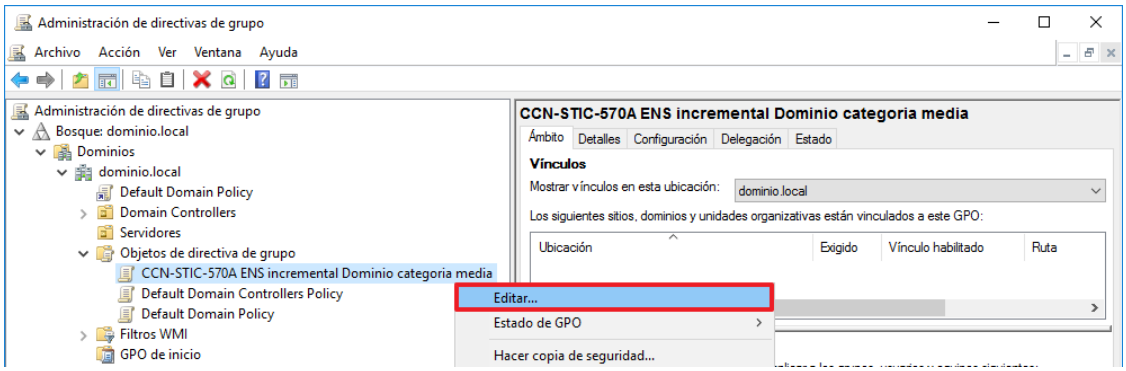
1. PREPARACIÓN DE DOMINIO

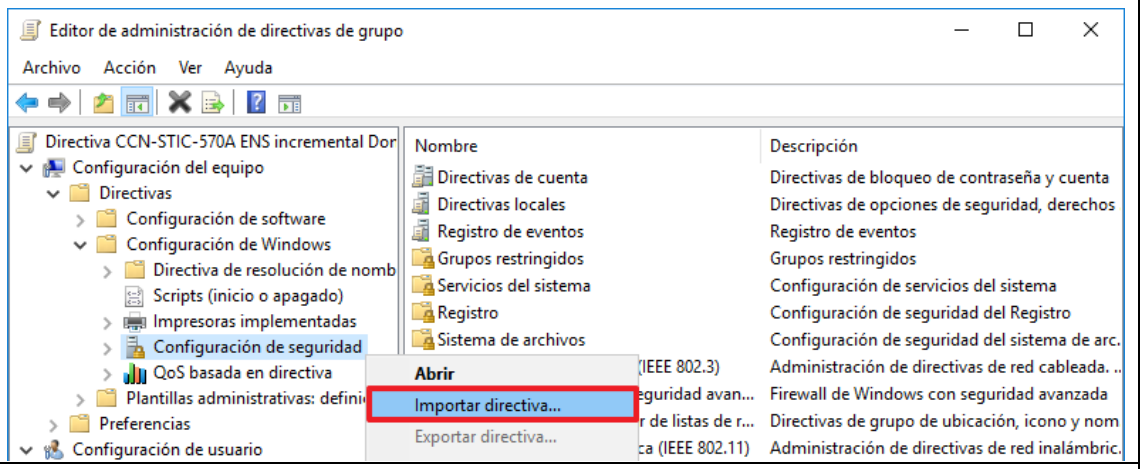
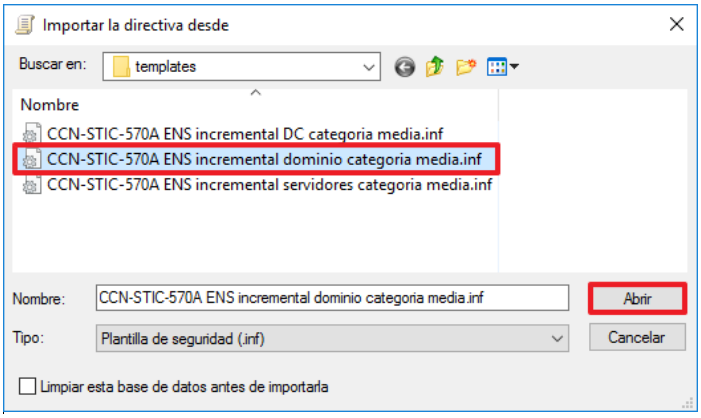
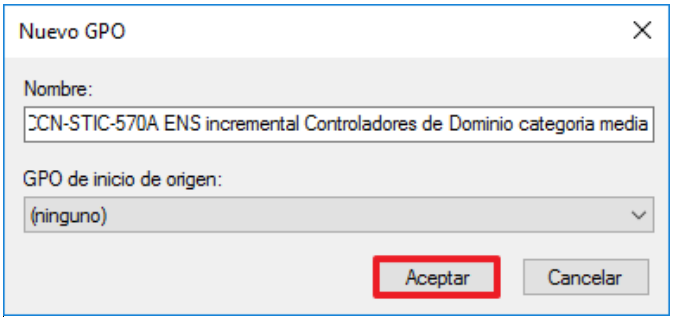
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se realizará la implementación de las plantillas de seguridad. Solo es necesario realizar este procedimiento una vez.

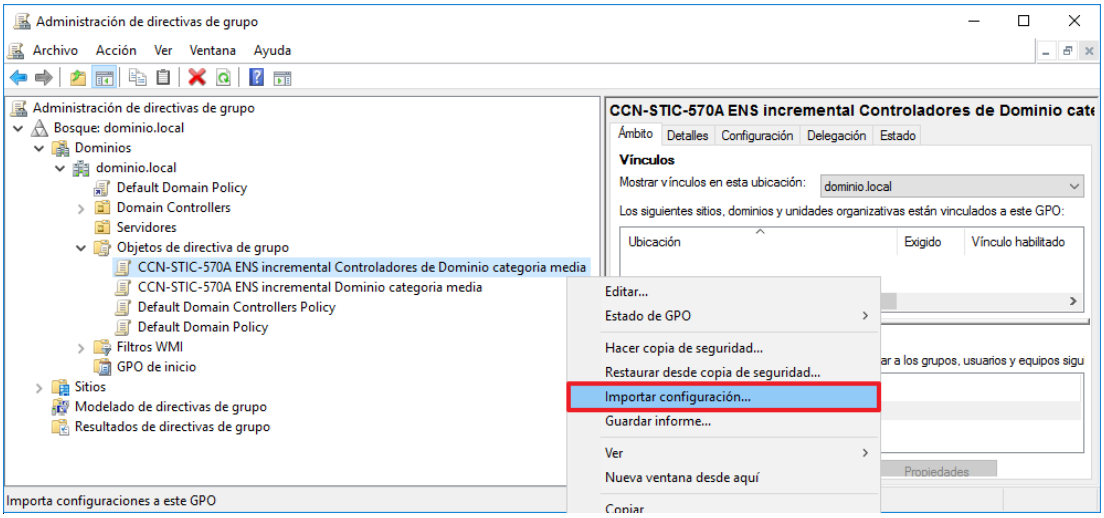
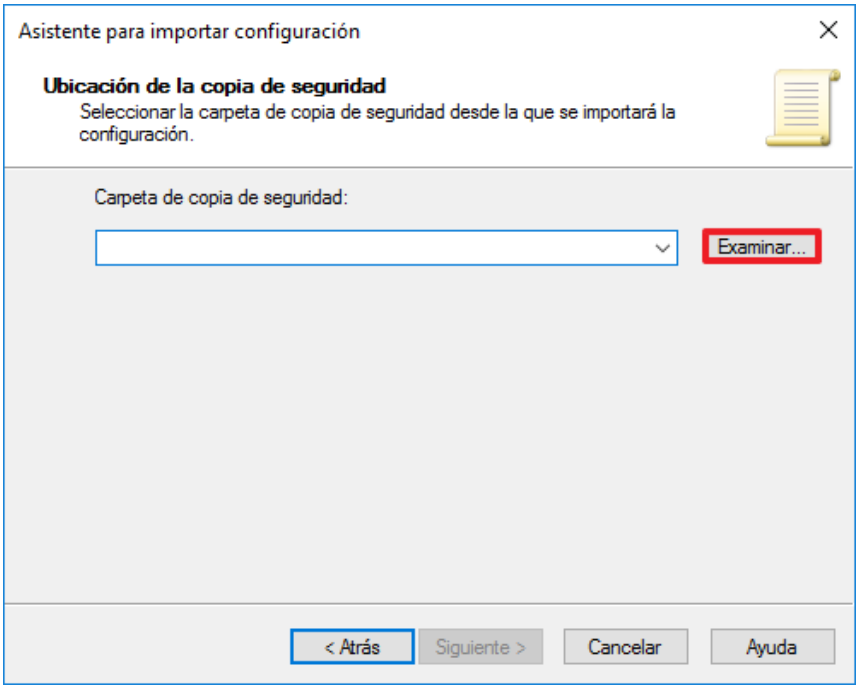
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Cree el directorio “Scripts” en la unidad C:\.
4.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts". **Nota:** Los recursos asociados a esta guía se encuentran en el directorio “Scripts-570A”.

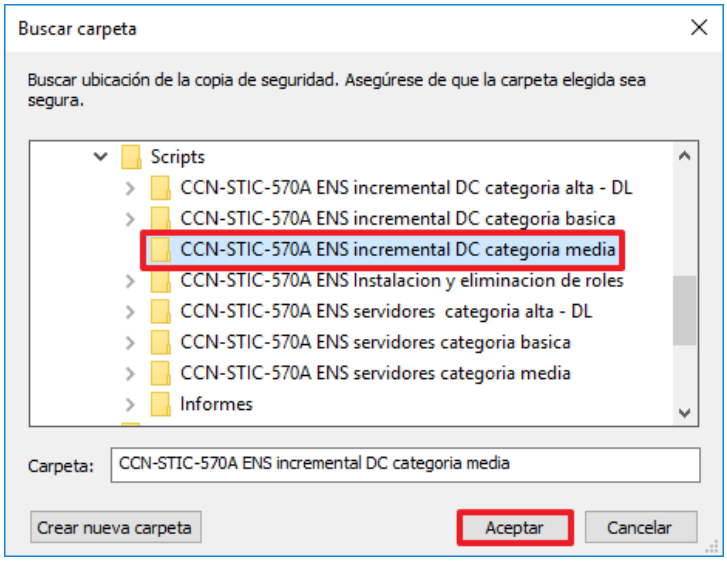
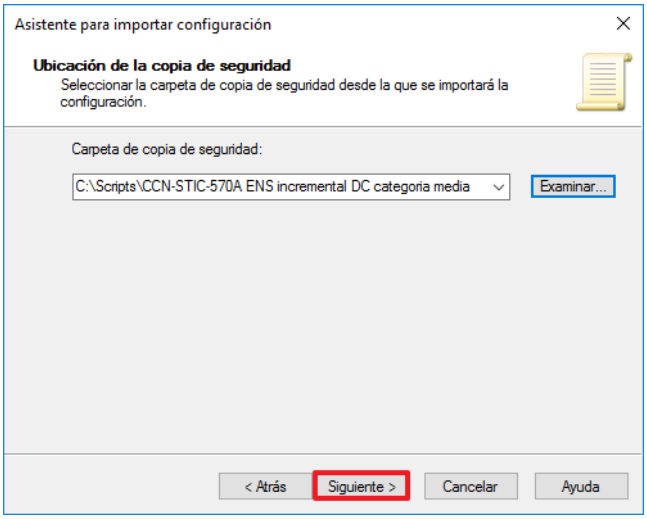
Paso	Descripción
5.	Configure el "Explorador de archivos" para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos" oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de "Inicio" con el botón derecho y seleccione "Explorador de archivos". 
6.	En el "Explorador de archivos" pulse sobre la pestaña "Vista" del menú superior y seleccione el icono de "Opciones". 
7.	En "Opciones de carpeta" sitúese en la pestaña "Ver" y en el campo "Configuración avanzada" localice y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos". Pulse primero sobre el botón "Aplicar", después sobre "Aplicar a las carpetas" (Pulse "Sí" ante el mensaje de confirmación) y, por último, pulse "Aceptar". 

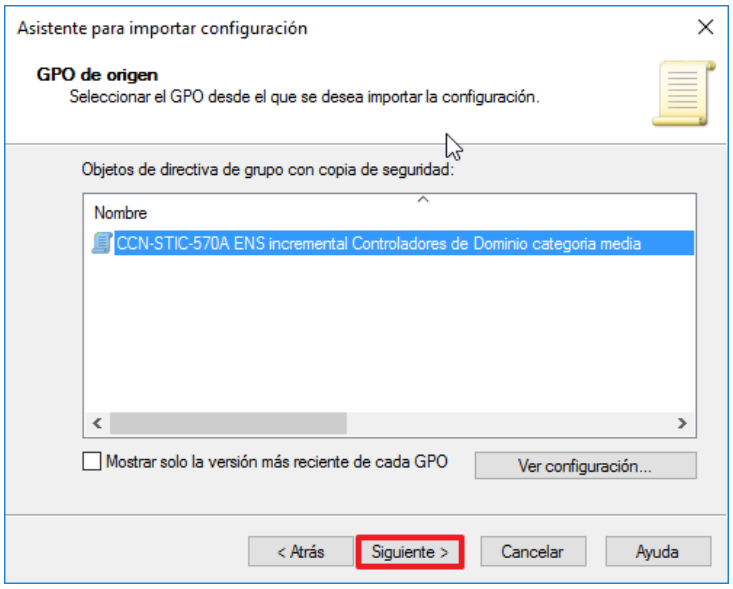
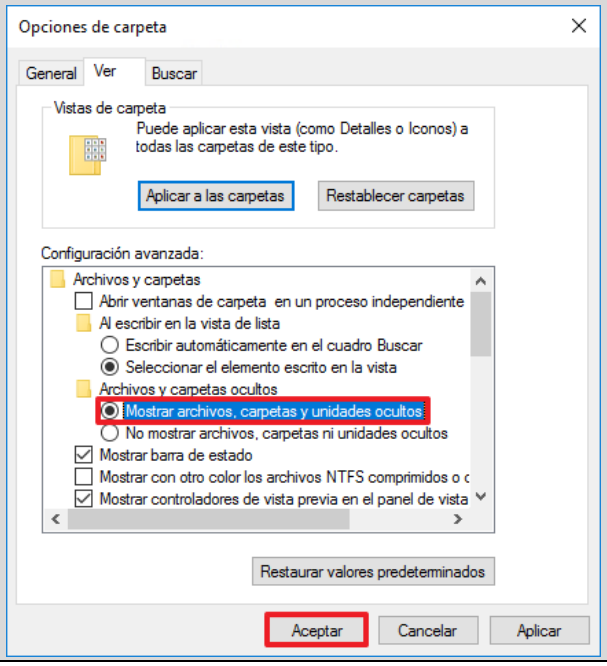
Paso	Descripción
8.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio: – CCN-STIC-570A ENS incremental DC categoria media (directorio) – CCN-STIC-570A ENS servidores categoria media (directorio) – CCN-STIC-570A ENS incremental DC categoria media.inf – CCN-STIC-570A ENS incremental dominio categoria media.inf – CCN-STIC-570A ENS Incremental servidores categoria media.inf
9.	Copie los ficheros “CCN-STIC-570A ENS incremental dominio categoria media.inf” y “CCN-STIC-570A ENS incremental DC categoria media.inf, al directorio “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Según la configuración de seguridad de UAC, el sistema podría solicitar la elevación de privilegios, en este caso, pulse “Continuar”. 
10.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”** 
11.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”.

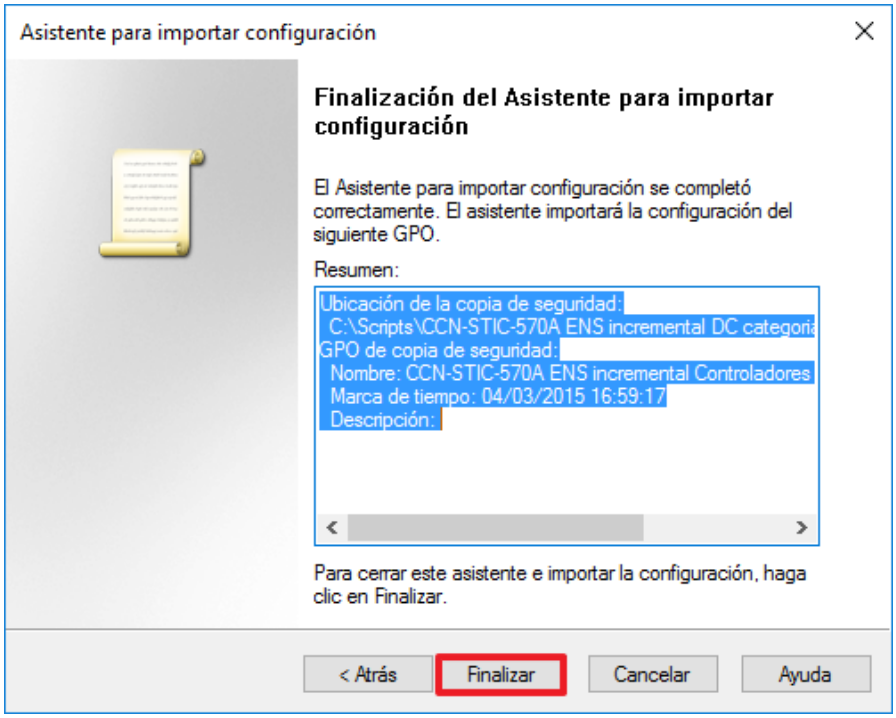
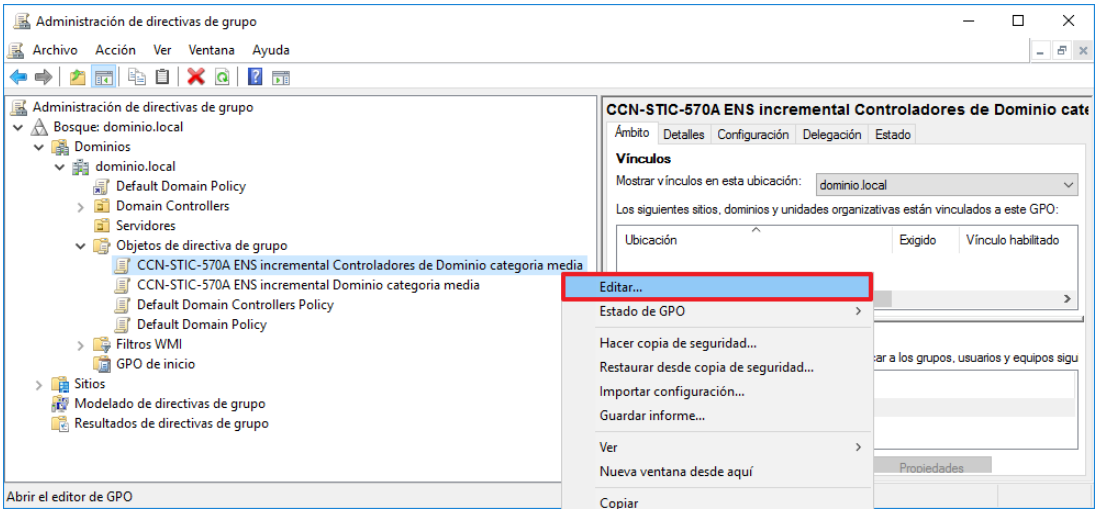
Paso	Descripción
12.	Pulse con el botón derecho, sobre dicha y carpeta y seleccione la opción “Nuevo”. 
13.	Introduzca como nombre “CCN-STIC-570A ENS incremental Dominio categoria media” y pulse el botón “Aceptar”. 
14.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
15.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**

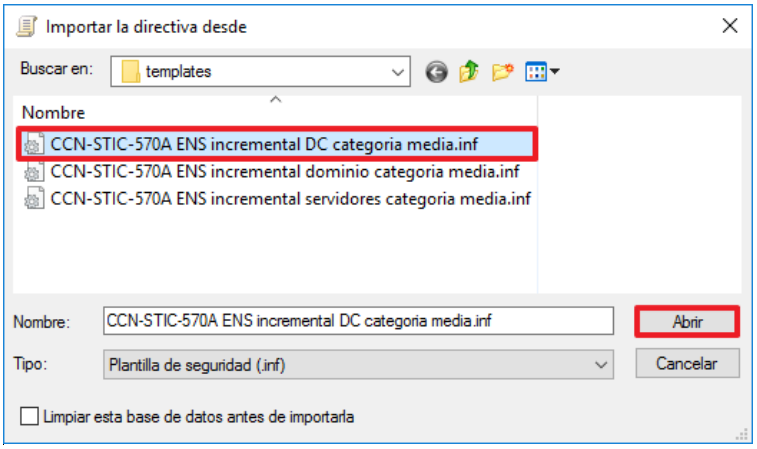
Paso	Descripción
16.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva…”. 
17.	Seleccione de la ruta “C:\Windows\Security\Templates” el fichero “CCN-STIC-570A ENS incremental Dominio categoria media” y pulse el botón “Abrir”. 
18.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
19.	Vuelva a pulsar con el botón derecho sobre el contenedor de objetos de directiva de grupo y seleccione la opción “Nuevo”.
20.	Introduzca como nombre “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media” y pulse el botón “Aceptar”. 

Paso	Descripción
21.	La nueva política requiere una configuración de plantillas administrativas. Para ello y seleccionando la política, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración…”. 
22.	En el asistente de importación de configuración, pulse el botón “Siguiente >”.
23.	En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.
24.	En “Carpeta de copia de seguridad”, pulse el botón “Examinar...”. 

Paso	Descripción
25.	Seleccione la carpeta “CCN-STIC-570A ENS incremental DC categoria media” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 
26.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada. 

Paso	Descripción
27.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-570A incremental Controladores de Dominio categoria media” y pulse el botón “Siguiente >”.  **Nota:** Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero “manifest.xml”. Este es un fichero oculto y, por lo tanto, debe mostrar en “opciones de carpeta” la opción “Mostrar archivos, carpetas y unidades ocultos”. 
28.	En la pantalla de examen, pulse el botón “Siguiente >”.

Paso	Descripción
29.	Para completar el asistente pulse el botón “Finalizar”. 
30.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración.
31.	A continuación, seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
32.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**
33.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva…”.

Paso	Descripción
34.	Seleccione de la ruta “C:\Windows\Security\Templates” el fichero “CCN-STIC-570A ENS incremental DC categoria media” y pulse el botón “Abrir”. 
35.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
36.	Las políticas se encuentran ya creadas correctamente. No obstante, no se aplicarán hasta más adelante, una vez que haya tenido en cuenta y aplicado todas las consideraciones adicionales que se mostrarán en el siguiente punto del presente anexo. Cierre la herramienta “Administración de Directivas de Grupo”.

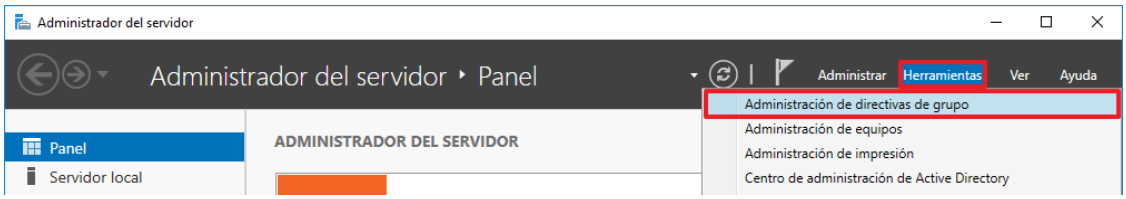
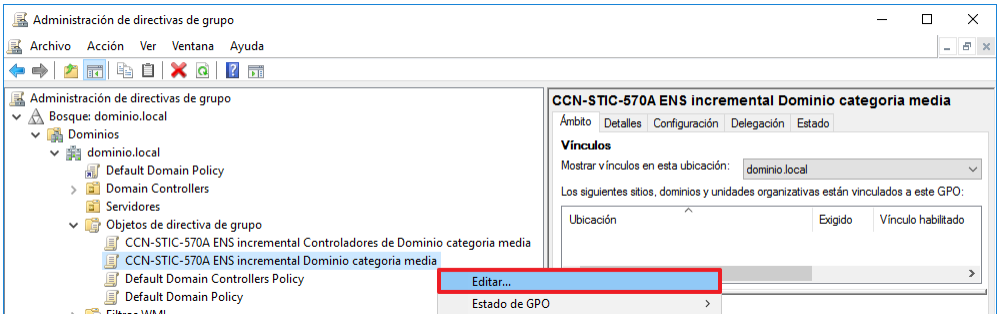
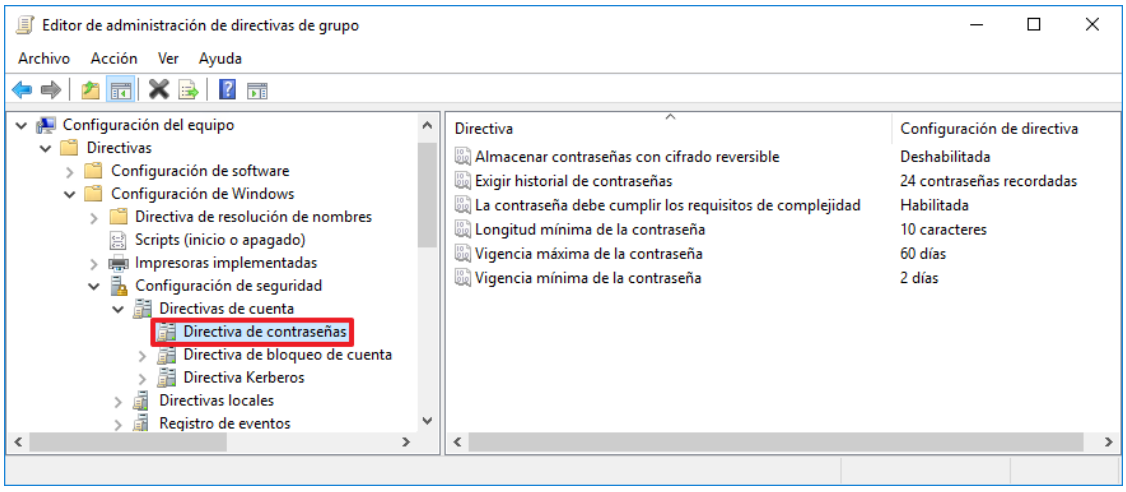
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

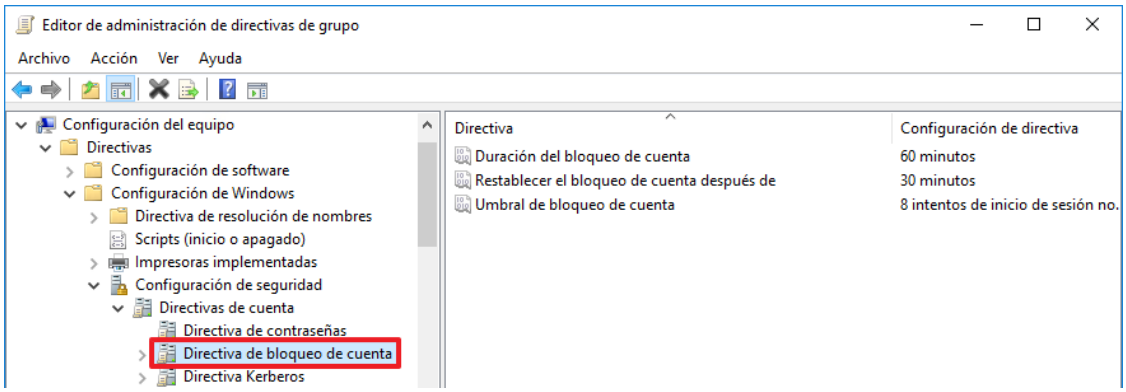
El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración. Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría media. No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

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

2.1. CONTRASEÑAS Y BLOQUEO DE CUENTAS

Es factible que su organización cuente con una política de contraseña consolidada. La implementación de la política que se aplicará sobre el dominio "CCN-STIC-570A ENS incremental Dominio categoria media" aplicará una de forma particular. Deberá evaluarla para determinar si esta configuración le es válida o por el contrario debe adaptarla a las condiciones de su organización.

Paso	Descripción
37.	Para evaluar y realizar la modificación oportuna inicie la herramienta "Administración de Directivas de Grupo". Para ello y sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"** 
38.	Edite el objeto de GPO "CCN-STIC-570A ENS incremental Dominio categoria media". Para ello seleccione dicha política y seleccione la opción "Editar…". 
39.	Despliegue la política y sitúese en la siguiente ruta: **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseñas"** 

Paso	Descripción
40.	Evalúe la política de contraseñas y modifíquela convenientemente. **Nota:** Debe tener en consideración que si su política de credenciales es menos rigurosa que la marcada en la configuración deseada, se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de contraseñas a lo marcado por la configuración recomendada.
41.	De forma similar a lo anterior, deberá evaluar la política de bloqueo de cuenta. Para ello y sin cerrar la política, seleccione la "Directiva de bloqueo de cuenta" que encontrará al mismo nivel que la directiva de contraseñas. 
42.	Evalúe la política de bloqueo de cuenta y modifíquela convenientemente. **Nota:** Debe tener en consideración que, si su política de bloqueo de cuenta es menos rigurosa que la marcada en la configuración deseada, se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de bloqueo de cuenta a lo marcado por la configuración recomendada.
43.	Cierre el "Editor de administración de directivas de grupo".
44.	Cierre la herramienta "Administración de directivas de grupo".

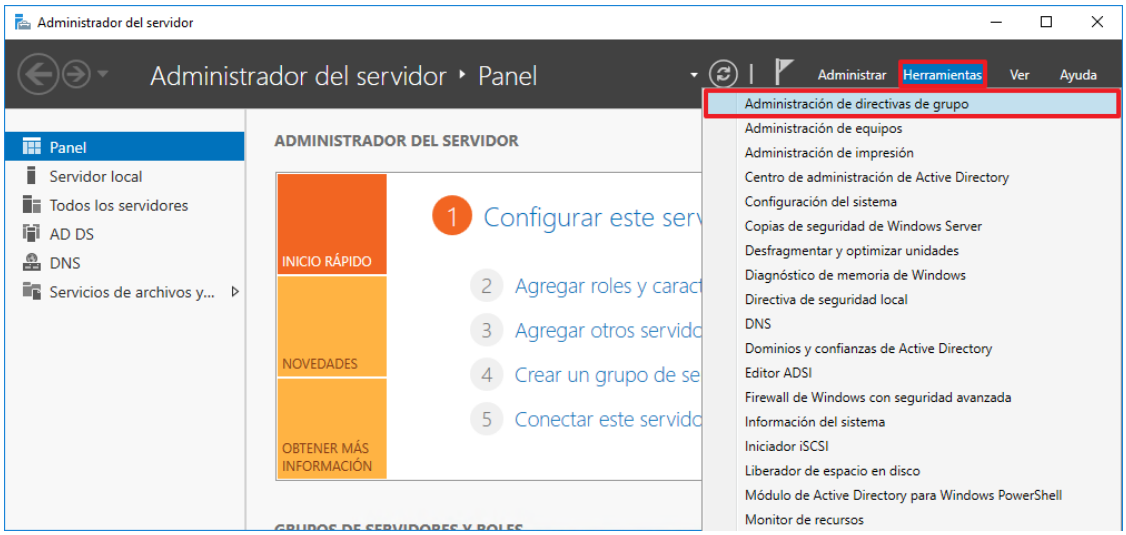
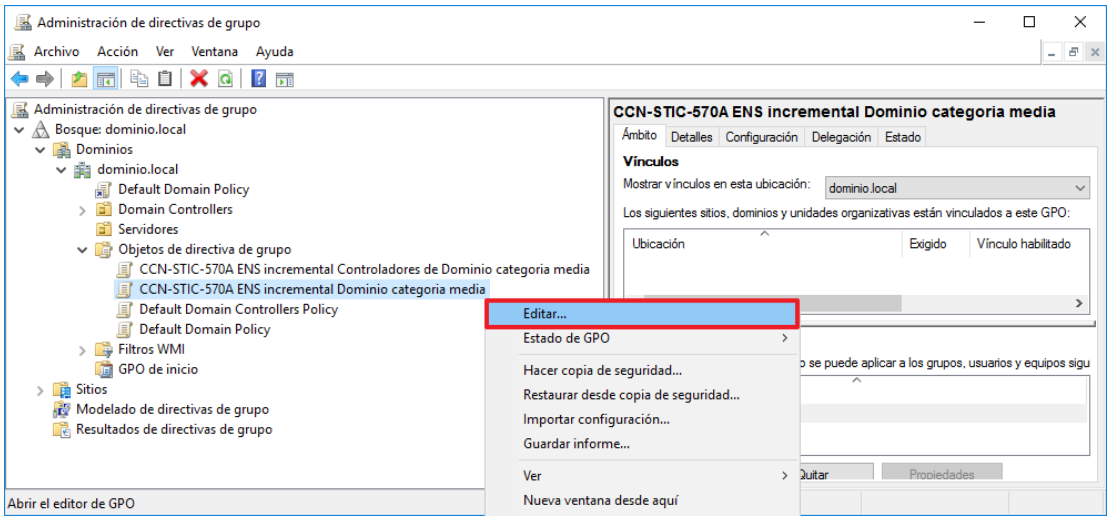
2.2. INFORMACIÓN DE OBLIGACIONES

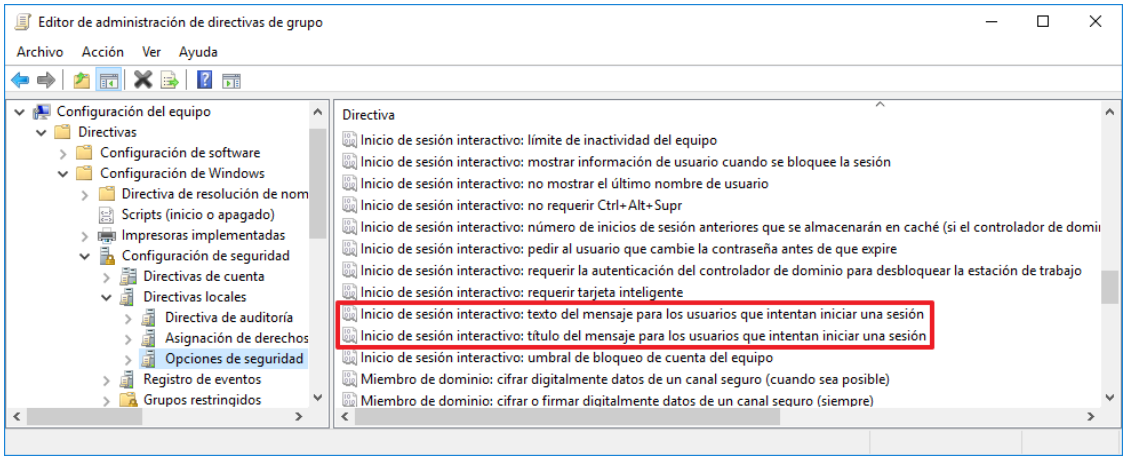
Uno de los aspectos que marca el ENS desde su requisito de categoría baja en el Marco Operacional para el acceso local, consiste en la necesidad de informar al usuario de sus obligaciones.

Los sistemas Windows presentan mecanismos para implementar mensajes que realizan advertencias al usuario cuando va a realizar el inicio de la sesión. Aunque pudieran emplearse otros tales como la ejecución de scripts, el empleo de este mecanismo es altamente recomendable. Debe, no obstante, tomarse en consideración que su organización ya está empleando este mecanismo para notificar otros detalles como los marcados por el Reglamento Europeo General de Protección de Datos (GDPR) 2016/679/CE y la Ley Orgánica 15/1999 de protección de datos de carácter personal.

Si fuera así, modifique el mensaje mostrado para adaptarlo también al cumplimiento del ENS según lo estipulado en la política de seguridad de su organización.

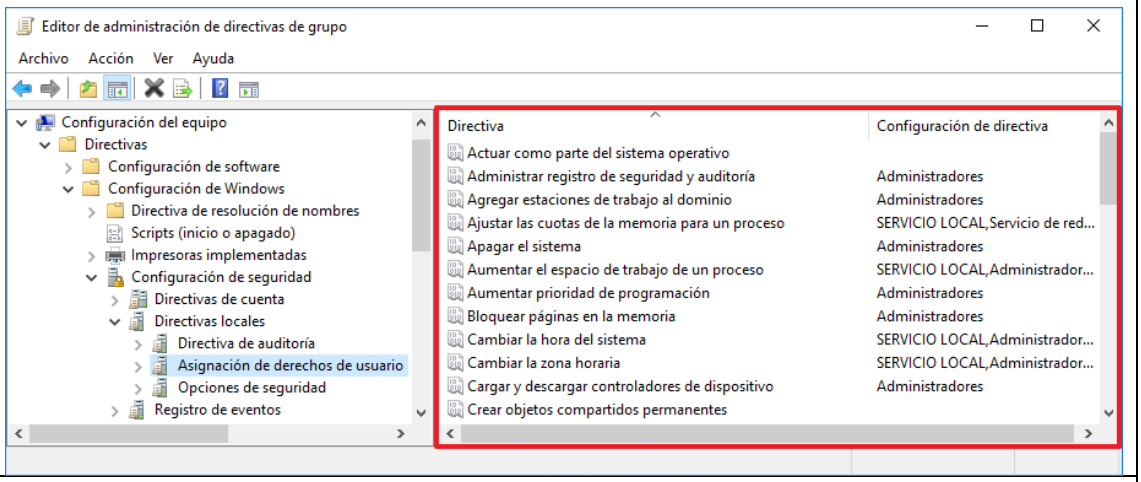
Si su organización no está haciendo uso de este mecanismo siga los siguientes pasos para habilitar el sistema de advertencia, con objeto de informar al usuario de sus obligaciones, según quede estipulado en la política de seguridad de la organización.

Paso	Descripción
45.	Inicie la herramienta "Administración de Directivas de Grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"** 
46.	Edite el objeto de GPO "CCN-STIC-570A ENS incremental Dominio categoria media". Para ello seleccione dicha política y seleccione la opción "Editar…". 
47.	Despliegue la política y sitúese en la siguiente ruta: **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"**

Paso	Descripción
48.	Identifique las directivas “Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión” e “Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión”. 
49.	Edite ambas directivas incluyendo el título de la advertencia y el mensaje a facilitar a los usuarios según se estipule en las políticas de seguridad de la organización.
50.	Cierre la política de seguridad.
51.	Cierre “Administración de Directivas de Grupo”.

2.3. ASIGNACIÓN DE DERECHOS DE USUARIO

Paso	Descripción
52.	Los objetos de políticas de grupo para Controladores de Dominio y Servidores miembros especifican unos derechos de usuario siguiendo planteamientos de seguridad que aplican los principios de mínimo privilegio y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les hayan asignado derechos determinados para la administración o gestión de los sistemas. Si esto fuera así, deberá realizar las modificaciones pertinentes sobre el objeto de política de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.
53.	Edite la política de grupo correspondiente iniciando la herramienta “Administración de Directivas de Grupo” y seleccionando la política a modificar. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”** Sobre el objeto de GPO que se quiere modificar, deberá pulsar clic derecho y seleccionar “Editar” en el menú desplegado.

Paso	Descripción
54.	Una vez abierto el "Editor de administración de directivas de grupo", despliegue la política y sitúese en la siguiente ruta: **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"** 
55.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
56.	Guarde la configuración cerrando la ventana de editor de administración de directivas de grupo.

2.4. BLOQUEO DE SESIÓN ANTE INACTIVIDAD

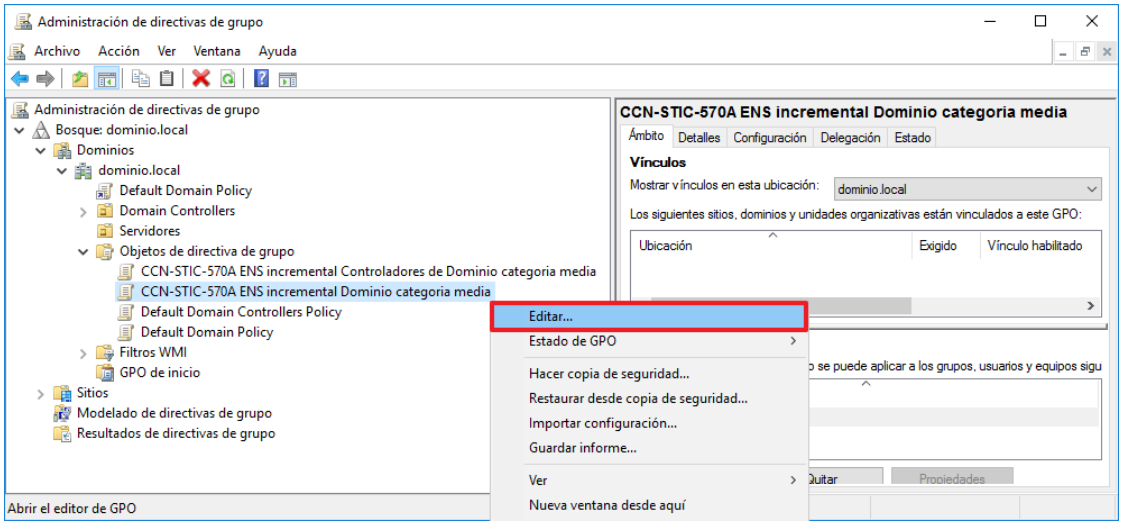
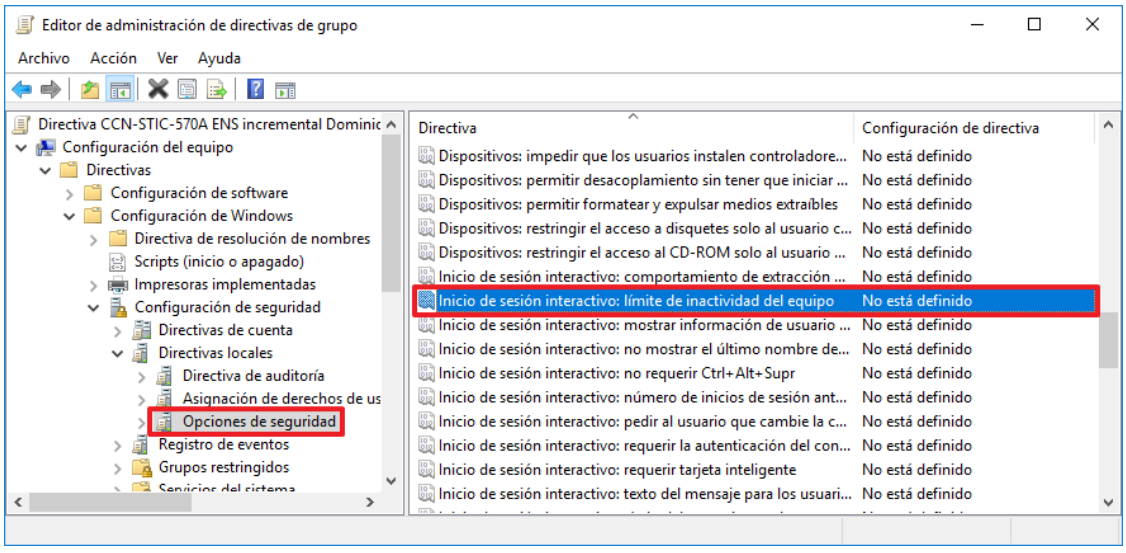
Se establece, a partir de la categoría media y según MP. EQ. 2, la necesidad de realizar el bloqueo del equipo ante un tiempo razonable de inactividad. A través de las políticas de grupo aplicables sobre el usuario, puede establecerse la medida de protección que habilita el salvapantallas y, por lo tanto, el bloqueo de la sesión.

La implementación de esta medida puede realizarse a través de estrategias diferentes. La presente guía determina la aplicación a todo el dominio modificando la política de dominio. No obstante, también podría determinarse crear una política nueva que, aplicable a nivel del dominio, solo fuera efectiva a un grupo de usuarios concretos.

Debe tener en consideración que la política de bloqueo por salvapantallas se aplica a través de GPO por usuario y no por equipo.

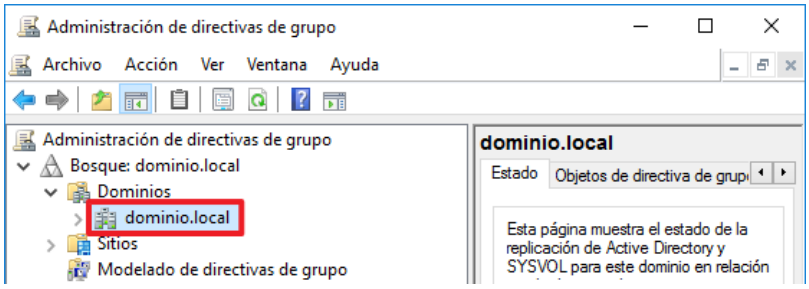
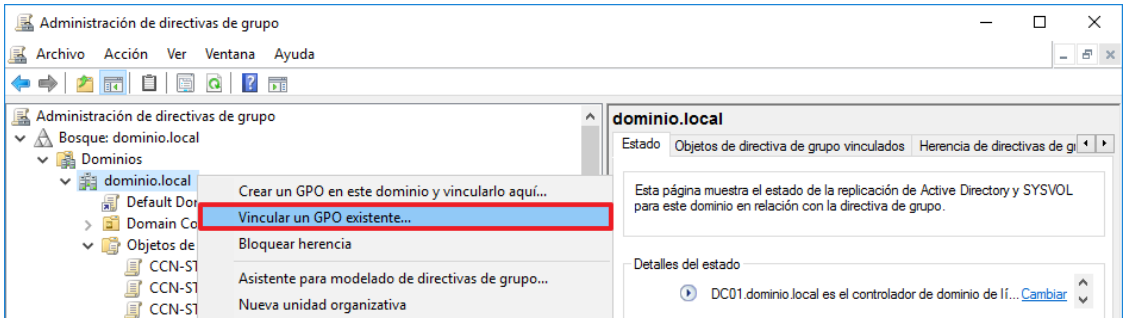
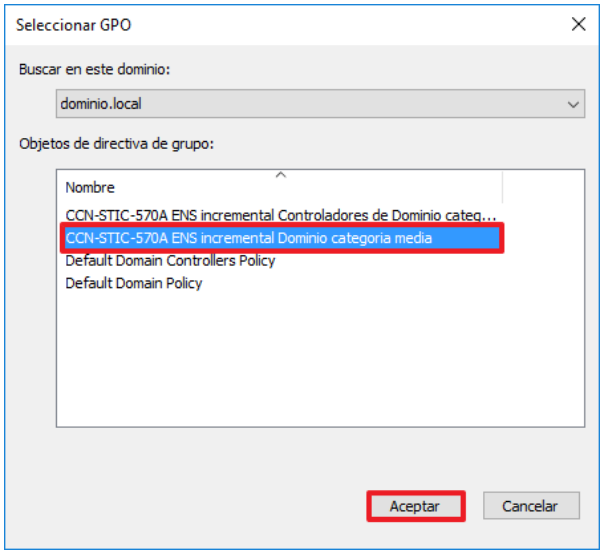
Si la organización presenta mecanismos para realizar el bloqueo del equipo ante inactividad no es necesario que aplique la siguiente configuración. No obstante, revise la configuración para adaptarse a la normativa vigente. Si la organización no tiene medidas dispuestas siga los siguientes pasos.

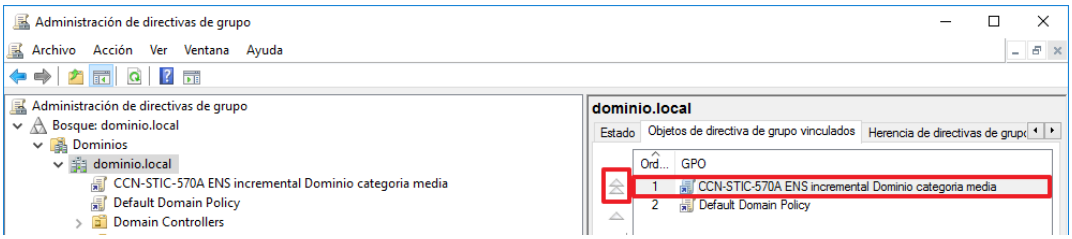
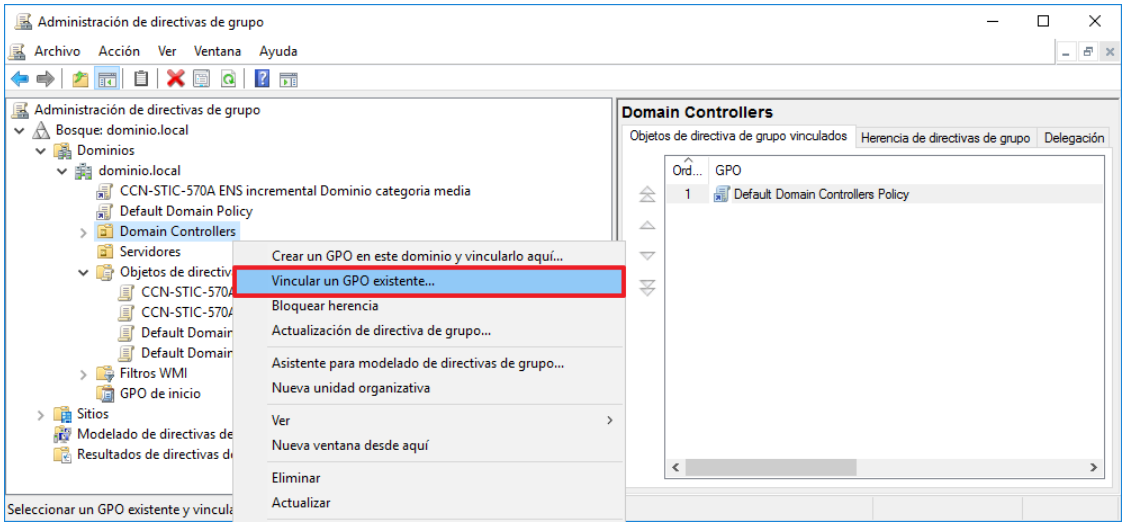
Paso	Descripción
57.	Para evaluar y realizar la modificación oportuna inicie la herramienta "Administración de directivas de grupo".

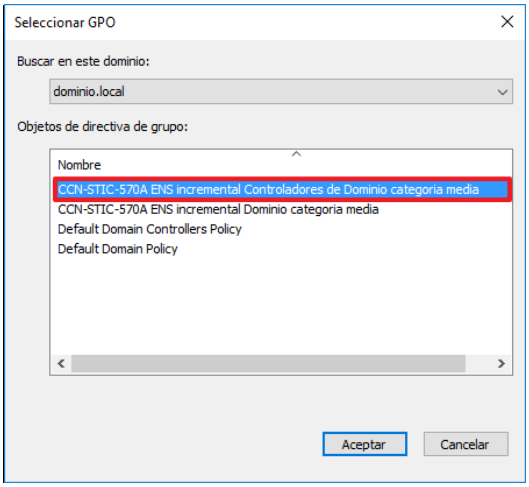
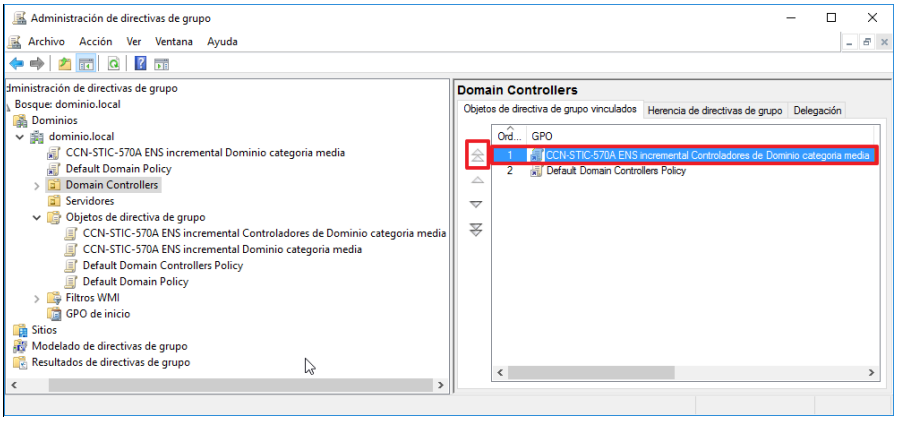
Paso	Descripción
58.	Edite el objeto de GPO “CCN-STIC-570A ENS incremental Dominio categoria media”. Para ello seleccione dicha política y seleccione la opción “Editar…”. 
59.	Despliegue la política y sitúese en la siguiente ruta: **“Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”** Habilite y configure la directiva de seguridad: – Inicio de sesión interactivo: límite de inactividad del equipo Establezca el valor en 600 segundos (10 minutos). 
60.	Cierre la política.

3. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

El presente punto establece la aplicación de las políticas de seguridad, toda vez que se han tenido en consideración las condiciones definidas en el punto previo.

Paso	Descripción
61.	Inicie la herramienta de administración de directivas de grupo.
62.	Despliegue el bloque y posiciónese sobre su dominio.  **Nota:** En el ejemplo el dominio utilizado se denomina “dominio.local”.
63.	Pulse con el botón derecho sobre el mismo y seleccione la opción “Vincular un GPO existente…”. 
64.	Seleccione la política “CCN-STIC-570A ENS incremental Dominio categoria media” y pulse el botón “Aceptar”. 

Paso	Descripción
65.	Una vez agregado, en el panel derecho seleccione la pestaña “Objetos de directiva de grupo vinculados” y seleccione la política “CCN-STIC 570A ENS incremental Dominio categoria media”
66.	Pulse el botón con la flecha que apunta hacia arriba hasta situar la política “CCN-STIC 570A ENS incremental Dominio categoria media” en primer lugar dentro del orden de vínculo. 
67.	Seleccione la Unidad Organizativa “Domain Controllers” y seleccione la opción “Vincular un GPO existente…”.  **Nota:** Si sus controladores de dominio se encontrarán en otra ubicación vincule la siguiente GPO en dicha OU.

Paso	Descripción
68.	Seleccione la política “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media” y pulse el botón “Aceptar”. 
69.	Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media” y pulse el botón con la flecha que apunta hacia arriba hasta situarla en primer lugar dentro del orden de vínculo. 
70.	Cierre la herramienta de administración de directivas de grupo.
71.	Elimine la carpeta “C:\Scripts”.

4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD EN LOS EQUIPOS

Las configuraciones planteadas a través de la presente guía han sido ampliamente probadas en entornos de operativa Microsoft. No obstante, no se han podido probar todas las condiciones existentes, ni con las peculiaridades de cada organización. Bajo determinadas condiciones, pudieran suceder algunas incidencias que se describen a continuación, así como su resolución.

Debe tenerse en consideración que la resolución consiste en rebajar algunos de los mecanismos de seguridad descritos en la presente guía. Por lo tanto, deberá plantearse una

solución que, de forma paulatina, permita alcanzar el estado de seguridad deseado y recomendado por la presente guía.

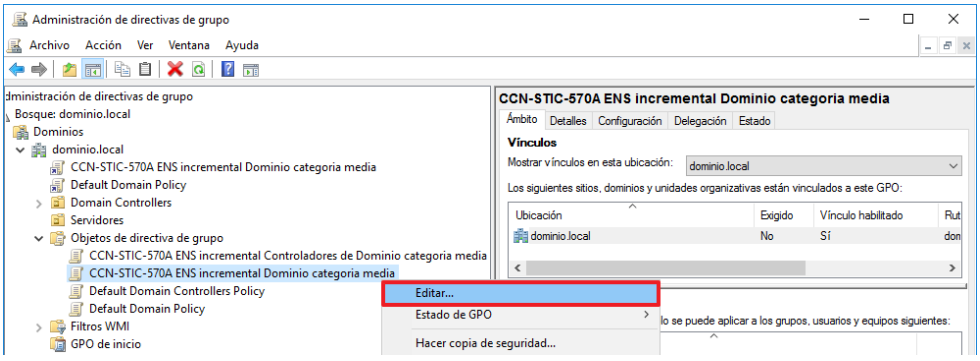
4.1. CIFRADOS PERMITIDOS PARA KERBEROS

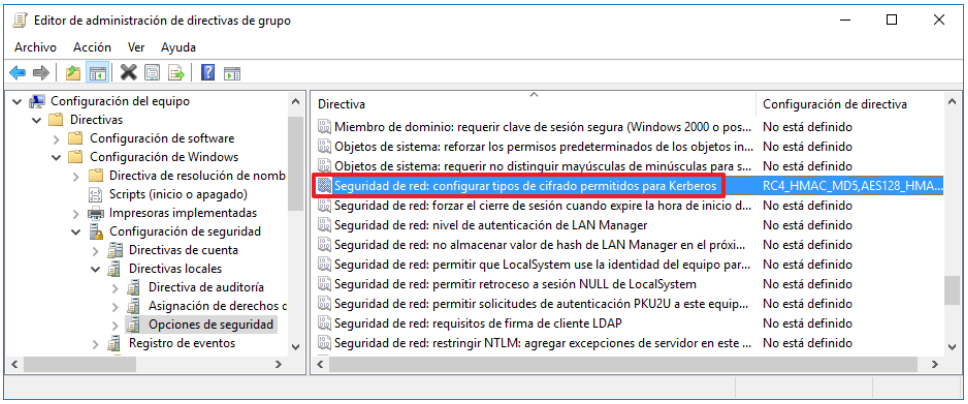
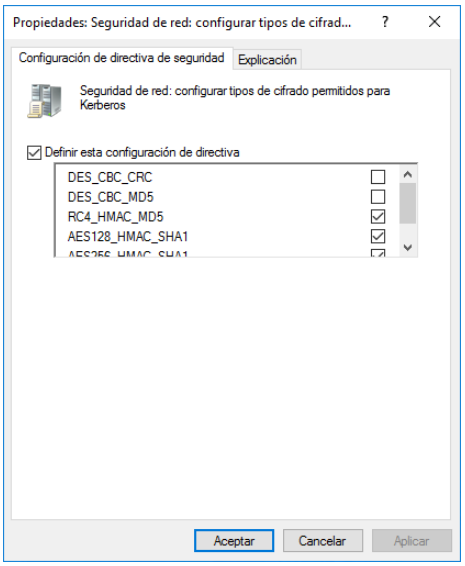
Un elemento significativo para los procesos de autenticación, en el marco de un dominio, lo corresponde la autenticación Kerberos. El proceso de validación se realiza mediante sistemas que garantizan la confidencialidad e integridad de la información transmitida. No obstante, debe tenerse en consideración que no todos los algoritmos admitidos por Microsoft son seguros y, por lo tanto, no serían compatibles con la seguridad planteada a través del Esquema Nacional de Seguridad. La política de seguridad de dominio para la categoría media presenta una implementación de mínimos adecuados con los requisitos de seguridad. No obstante, las pruebas efectuadas en laboratorio han permitido determinar que el empleo de determinados clientes o servidores Linux, o bien la integración con sistemas operativos Microsoft ya obsoletos, pudiera ser incompatible con la configuración establecida.

También pudieran darse problemas de comunicación ante determinadas relaciones entre diferentes árboles de un mismo bosque que han ido evolucionando desde dominios Windows NT, Windows 2000, Windows 2003 o Windows 2008.

Nota: Tenga en consideración que Windows Server 2016 ya no está soportado para trabajar a nivel funcional de Windows Server 2003, por lo que deberá actualizar su infraestructura para que el nivel funcional sea superior a 2003.

En caso de identificar problemas de validación de equipos previos a Windows XP o equipos no Microsoft, o bien entre dominio o árboles de un mismo bosque cuando ponga en producción la política de dominio “CCN-STIC-570A ENS incremental Dominio categoria media”, se deberá realizar una modificación sobre la misma.

Paso	Descripción
72.	Para evaluar y realizar la modificación oportuna inicie la herramienta de “Administración de directivas de grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**
73.	Edite el objeto de GPO “CCN-STIC-570A ENS incremental Dominio categoria media”. Para ello seleccione dicha política y seleccione la opción “Editar…”. 
74.	Despliegue la política y sitúese en la siguiente ruta: **“Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**

Paso	Descripción
75.	Identifique la directiva “Seguridad de red: configurar tipos de cifrado permitidos para Kerberos”. 
76.	Edítela pulsando doble clic sobre la misma. La configuración predeterminada de seguridad para el cumplimiento de ENS en su categoría media, es la siguiente. 
77.	Active el resto de opciones pulsando sobre los recuadros que no están marcados y cierre la política mediante el botón “Aceptar”.
78.	Aplique, a posteriori, la nueva configuración para evaluar si se han resuelto las incidencias identificadas. **Nota:** Debe tener en consideración que, si ha implementado algoritmos de seguridad alternativos a los propuestos en la configuración deseada de esta guía, se encuentra por debajo de los requerimientos de seguridad actuales. Debería evaluar a qué se deben dichas incidencias y resolverlas para volver a un estado de seguridad adecuado. Es factible que los procesos de autenticación Kerberos para determinados sistemas requieran de algoritmos débiles y pueda encontrarse ante riesgos de seguridad significativos para la organización exponiéndose, por ejemplo, a ataques de tipo *man in the middle* contra los procesos de autenticación en el dominio.

ANEXO A.3.2. LISTA DE COMPROBACIÓN DE WINDOWS SERVER 2016 COMO CONTROLADOR DE DOMINIO PARA LA CATEGOÍA MEDIA

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía "ANEXO A.3.1 GUÍA PASO A PASO CONTROLADOR DE DOMINIO QUE LE SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS".

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los dominios y servidores Windows Server 2016 con implementación de seguridad de categoría media del ENS.

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

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

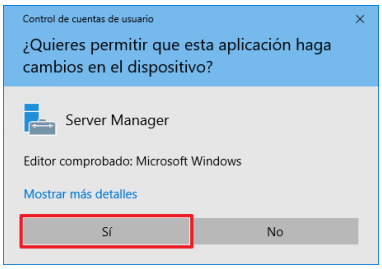
b) Conjunto resultante de directivas (rsop.msc).

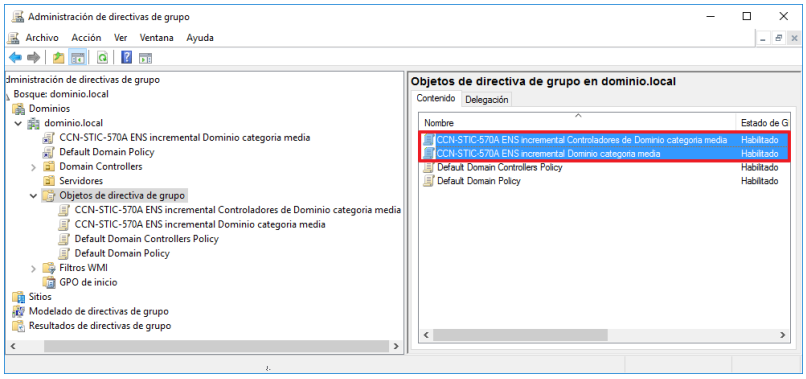
c) Consola de servicios (services.msc).

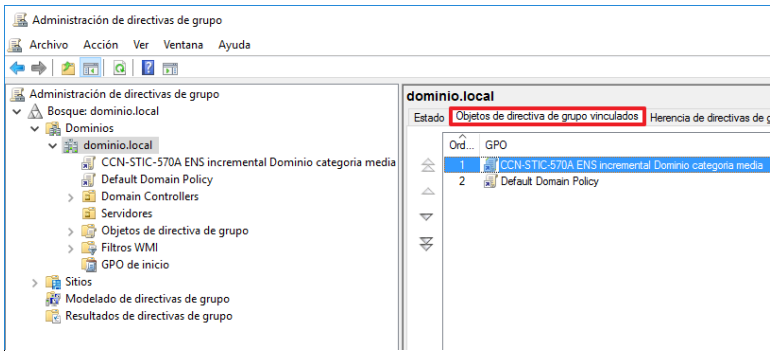
d) Editor de registro (regedit.exe).

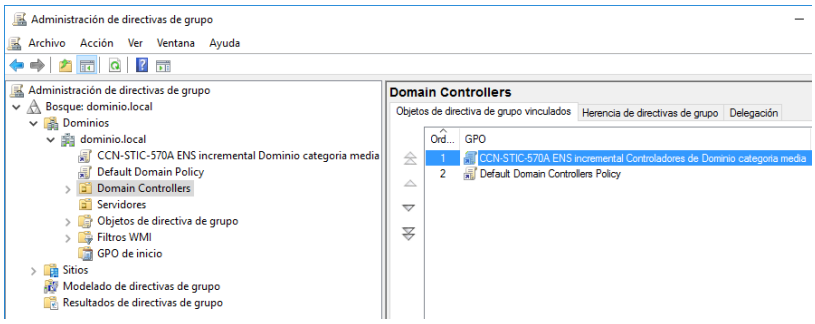
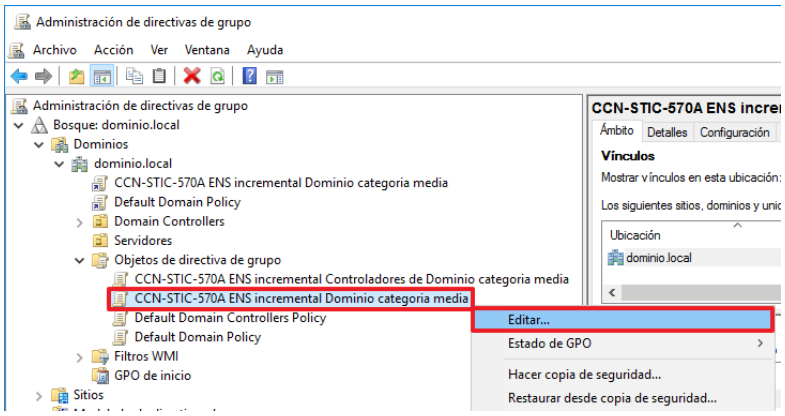
e) Explorador de Archivos (explorer.exe).

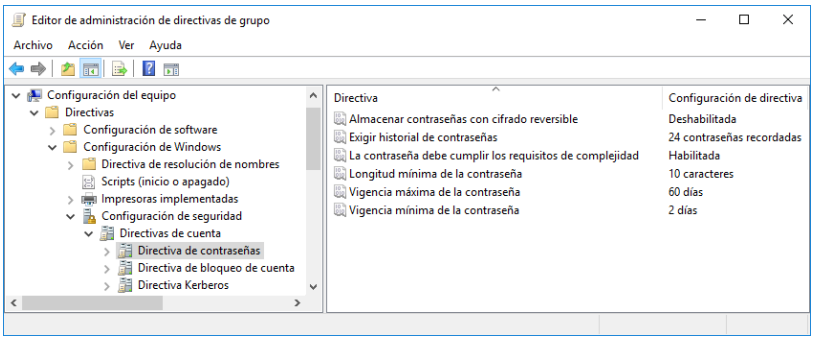
f) Usuarios y equipos de Active Directory (dsa.msc).

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. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Pulse "Sí" en la ventana de "Control de cuentas de usuario". 
2. Verifique que los objetos de directivas de grupo han sido creados y están habilitados.		Ejecute la herramienta "Administrador de directivas de grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"** 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>Dentro de la consola diríjase a los “Objetos de directiva de grupo”:
“Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo”
Verifique que están creados los dos objetos de directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media” y “CCN-STIC-570A ENS incremental Dominio categoria media”, y que en la columna “Estado de GPO” figuran como habilitadas.
 

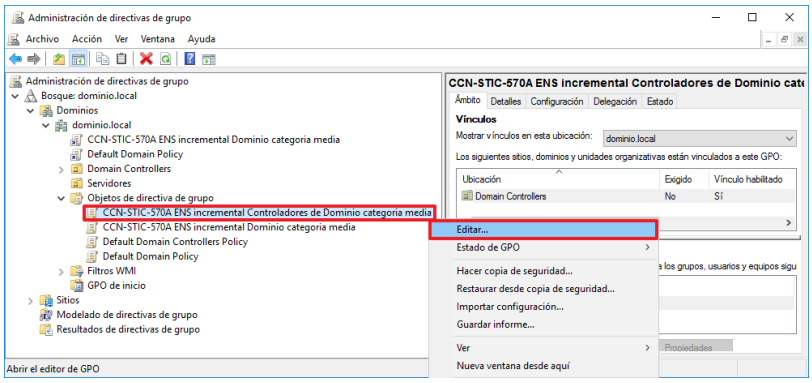
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-570A ENS incremental Controladores de Dominio categoria media</td><td>Habilitado</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS incremental Dominio categoria media</td><td>Habilitado</td><td></td></tr>
</table></td></tr>
<tr><td>3. Verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Dominio categoria media” aplica a todos los objetos del dominio y ocupa el primer lugar en el orden de vinculación.</td><td></td><td>En el árbol de la izquierda sitúese sobre el dominio desde:
“Bosque: [Su Bosque] → Dominios → [Su Dominio]”
En la pestaña “Objetos de Directiva de grupo vinculados” verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Dominio categoria media” figura en el panel de la derecha y ocupa el primer lugar en la columna “Orden de Vínculos”.
 
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
4. Verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Controladores de dominio categoria media” aplica a todos los objetos del contenedor “Domain Controllers” y ocupa el primer lugar en el orden de vinculación.		En el árbol de la izquierda sitúese sobre el contenedor “Domain Controllers” desde: **“Bosque: [Su Bosque] → Dominios → [Su Dominio] → Domain Controllers”** En la pestaña “Objetos de Directiva de grupo vinculados” verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Controladores de dominio categoria media” figura en el panel de la derecha y ocupa el primer lugar en la columna “Orden de Vínculos”. 
5. Verifique la directiva de contraseñas en el objeto de directiva “CCN-STIC-570A ENS incremental Dominio categoria media”.		En el “Administrador de Directivas de Grupo” pulse el botón derecho del ratón sobre la directiva desde: **“Bosque: [Su Bosque] → Dominios → [Su Dominio] → CCN-STIC-570A ENS incremental Dominio categoria media”** Seleccione la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de contraseñas”
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Almacenar contraseñas usando cifrado reversible</td><td>Deshabilitada</td><td></td></tr>
<tr><td>Exigir historial de contraseñas</td><td>24 contraseñas recordadas</td><td></td></tr>
<tr><td>Las contraseñas deben cumplir los requisitos de complejidad</td><td>Habilitada</td><td></td></tr>
<tr><td>Longitud mínima de la contraseña</td><td>10 caracteres</td><td></td></tr>
<tr><td>Vigencia máxima de la contraseña</td><td>60 días</td><td></td></tr>
<tr><td>Vigencia mínima de la contraseña</td><td>2 días</td><td></td></tr>
</table></td></tr>
<tr><td>6. Verifique las directivas de bloqueo de cuenta de la directiva de grupo “CCN-STIC-570A ENS incremental Dominio categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de bloqueo de cuenta”
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Duración del bloqueo de cuenta</td><td>60 minutos</td><td></td></tr>
<tr><td>Restablecer recuentos de bloqueo de cuenta tras</td><td>30 minutos</td><td></td></tr>
<tr><td>Umbral de bloqueo de cuenta</td><td>8 intentos de inicio de sesión no válidos</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>7. Verifique las directivas Kerberos en la directiva de grupo “CCN-STIC-570A ENS incremental Dominio categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva Kerberos”</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Aplicar restricciones de inicio de sesión de usuario</td><td>Habilitada</td><td></td></tr>
<tr><td>Tolerancia máxima para la sincronización de los relojes de los equipos</td><td>10 minutos</td><td></td></tr>
<tr><td>Vigencia máxima de renovación de vales de usuario</td><td>2 días</td><td></td></tr>
<tr><td>Vigencia máxima del vale de servicio</td><td>360 minutos</td><td></td></tr>
<tr><td>Vigencia máxima del vale de usuario</td><td>6 horas</td><td></td></tr>
</table>
</td></tr>
<tr><td>8. Verifique las opciones de seguridad de la directiva de grupo “CCN-STIC-570A ENS incremental Dominio categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas Locales → Opciones de seguridad”</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Acceso de red: permitir traducción SID/nombre anónima</td><td>Deshabilitada</td><td></td></tr>
<tr><td>Seguridad de red: configurar tipos de cifrado permitidos para Kerberos</td><td>DES_CBC_CRC (Deshabilitado)
DES_CBC_MD5 (Deshabilitado)
RC4_HMAC_MD5 (Habilitado)
AES128_HMAC_SHA1 (Habilitado)
AES256_HMAC_SHA1 (Habilitado)
Tipos de cifrado futuros (Habilitado)</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>9. Verifique las directivas de auditoría en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.</td><td></td><td>En el “Administrador de Directivas de Grupo” pulse el botón derecho del ratón sobre la directiva desde:
“Bosque: [Su Bosque] → Dominios → [Su Dominio] → Domain Controllers → CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”
Seleccione la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 

Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Auditar el acceso a objetos</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar el acceso del servicio de directorio</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar el cambio de directivas</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar el seguimiento de procesos</td><td>Sin auditoría</td><td></td></tr>
<tr><td>Auditar el uso de privilegios</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar eventos de inicio de sesión</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar eventos de inicio de sesión de cuenta</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar eventos del sistema</td><td>Correcto</td><td></td></tr>
<tr><td>Auditar la administración de cuentas</td><td>Correcto, Erróneo</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>10. Verifique la asignación de derechos de usuario en la directiva “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Administrar registro de seguridad y auditoría</td><td>Administradores</td><td></td></tr>
<tr><td>Agregar estaciones de trabajo al dominio</td><td>Administradores</td><td></td></tr>
<tr><td>Ajustar las cuotas de la memoria para un proceso</td><td>Administradores, SERVICIO LOCAL, Servicio de red</td><td></td></tr>
<tr><td>Apagar el sistema</td><td>Administradores</td><td></td></tr>
<tr><td>Aumentar el espacio de trabajo de un proceso</td><td>Administradores, SERVICIO LOCAL</td><td></td></tr>
<tr><td>Aumentar prioridad de programación</td><td>Administradores</td><td></td></tr>
<tr><td>Bloquear páginas en la memoria</td><td>Administradores</td><td></td></tr>
<tr><td>Cambiar la hora del sistema</td><td>SERVICIO LOCAL, Administradores</td><td></td></tr>
<tr><td>Cambiar la zona horaria</td><td>SERVICIO LOCAL, Administradores</td><td></td></tr>
<tr><td>Cargar y descargar controladores de dispositivo</td><td>Administradores</td><td></td></tr>
<tr><td>Crear objetos globales</td><td>Administradores, SERVICIO, SERVICIO LOCAL, Servicio de red</td><td></td></tr>
<tr><td>Crear un archivo de paginación</td><td>Administradores</td><td></td></tr>
<tr><td>Crear vínculos simbólicos</td><td>Administradores</td><td></td></tr>
<tr><td>Denegar el acceso desde la red a este equipo</td><td>ANONYMOUS LOGON, Invitados</td><td></td></tr>
<tr><td>Denegar el inicio de sesión como servicio</td><td>Invitados</td><td></td></tr>
<tr><td>Denegar el inicio de sesión como trabajo por lotes</td><td>Invitados</td><td></td></tr>
</table>
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Denegar el inicio de sesión localmente	Invitados	
		Denegar inicio de sesión a través de Servicios de Terminal Server	Invitados	
		Forzar cierre desde un sistema remoto	Administradores	
		Generar auditorías de seguridad	SERVICIO LOCAL, Servicio de red	
		Generar perfiles de un solo proceso	Administradores	
		Generar perfiles del rendimiento del sistema	Administradores	
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	Administradores	
		Hacer copias de seguridad de archivos y directorios	Administradores, Operadores de copia de seguridad	
		Modificar la etiqueta de un objeto	Administradores	
		Modificar valores de entorno firmware	Administradores	
		Permitir el inicio de sesión local	Administradores	
		Quitar equipo de la estación de acoplamiento	Administradores	
		Realizar tareas de mantenimiento de volumen	Administradores	
		Reemplazar un símbolo (token) de nivel de proceso	SERVICIO LOCAL, Servicio de red	
		Restaurar archivos y directorios	Administradores	
		Suplantar a un cliente tras la autenticación	Administradores, SERVICIO, SERVICIO LOCAL, Servicio de red	
		Tener acceso a este equipo desde la red	Administradores, Usuarios autentificados, ENTERPRISE DOMAIN CONTROLLERS	
		Tomar posesión de archivos y otros objetos	Administradores	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>11. Verifique las opciones de seguridad en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”</td></tr>
<tr><td></td><td colspan="2">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Acceso a redes: modelo de seguridad y uso compartido para cuentas locales</td><td>Clásico: usuarios locales se autentican con credenciales propias</td><td></td></tr>
<tr><td>Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos</td><td>Deshabilitada</td><td></td></tr>
<tr><td>Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: rutas del Registro accesibles remotamente</td><td>System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, Software\Microsoft\Windows NT\CurrentVersion</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th></th><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
	Acceso a redes: rutas y subrutas del Registro accesibles remotamente	Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib, System\CurrentControlSet\Services\SysmonLog	
	Acceso a red: permitir traducción SID/nombre anónima	Deshabilitada		
	Apagado: borrar el archivo de paginación de la memoria virtual	Habilitada		
	Apagado: permitir apagar el sistema sin tener que iniciar sesión	Deshabilitada		

	Directiva	Valor	OK/NOK
	Auditoría: apagar el sistema de	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
	inmediato si no se pueden registrar las auditorías de seguridad			
	Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitada		
	Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitada		
	Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada		
	Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitada		
	Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitada		
	Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitada		
	Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador	Pedir consentimiento		
	Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar	Pedir credenciales en el escritorio seguro		
	Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación	Habilitada		
	Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitada		

	Directiva	Valor	OK/NOK
	Control de cuentas de usuario: Modo de aprobación de	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo	
	administrador para la cuenta predefinida Administrador		
	Control de cuentas de usuario: Permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitada	
	Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de Registro en diferentes ubicaciones por usuario	Habilitada	
	Controlador de dominio: no permitir los cambios de contraseña de cuenta de equipo	Deshabilitada	
	Criptografía de sistema: forzar la protección con claves seguras para las claves de usuario almacenadas en el equipo	El usuario debe escribir una contraseña cada vez que use una clave.	
	Cuentas: estado de la cuenta de invitado	Deshabilitada	
	Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitada	
	DCOM: restricciones de acceso al equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)	O:BAG:BAD:(A;;CCDCLC;;;AU)(A;;CCDCLC;;;S-1-5-32-562)	
	DCOM: restricciones de inicio al equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)	O:BAG:BAD:(A;;CCDCLCSWRP;;;BA)(A;;CSW;;;AU)(A;;CCDCLCSWRP;;;S-1-5-32-562)	
	Dispositivos: impedir que los usuarios instalen controladores de impresora	Habilitada	
	Dispositivos: permitir desacoplamiento sin tener que iniciar sesión	Deshabilitada	
	Dispositivos: permitir formatear y expulsar medios extraíbles	Administradores	
	Directiva	**Valor**	**OK/NOK**
	Dispositivos: restringir el acceso a disquetes sólo al usuario con sesión iniciada localmente	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Dispositivos: restringir el acceso al CD-ROM sólo al usuario con sesión iniciada localmente	Habilitada	
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo	
		Inicio de sesión interactivo: mostrar información del usuario cuando se bloquee la sesión	No mostrar la información del usuario	
		Inicio de sesión interactivo: no mostrar el último nombre de usuario	Habilitada	
		Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr	Deshabilitada	
		Inicio de sesión interactivo: número de inicios de sesión anteriores que se almacenarán en caché (si el controlador de dominio no está disponible)	0 inicios de sesión	
		Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire	14 días	
		Inicio de sesión interactivo: requerir la autenticación del controlador de dominio para desbloquear la estación de trabajo	Habilitada	
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	
		Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitada	
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitada	
		Miembro de dominio: duración máxima de contraseña de cuenta de equipo	30 días	

	Directiva	Valor	OK/NOK
	Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	
	Miembro de dominio: requerir	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo	
	clave de sesión segura (Windows 2000 o posterior)		
	Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitada	
	Seguridad de red: nivel de autenticación de LAN Manager	Enviar sólo respuesta NTLMv2 y rechazar LM	
	Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada	
	Seguridad de red: permitir que LocalSystem use la identidad del equipo para NTLM	Habilitada	
	Seguridad de red: permitir retroceso a sesión NULL de LocalSystem	Deshabilitada	
	Seguridad de red: permitir solicitudes de autenticación PKU2U a este equipo para usar identidades en Internet.	Deshabilitada	
	Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma	
	Seguridad de red: restringir NTLM: auditar el tráfico NTLM entrante	Habilitar la auditoría para todas las cuentas	
	Seguridad de red: restringir NTLM: auditar la autenticación NTLM en este dominio	Habilitar todo	
	Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitada	
	Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada	

Directiva	Valor	OK/NOK
Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor	Requerido del cliente	
Servidor de red Microsoft: tiempo de inactividad requerido	15 minutos	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td></td><td colspan="2">antes de suspender la sesión</td><td></td><td></td></tr>
<tr><td rowspan="11">12. Verifique el registro de eventos en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro de Eventos”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Evitar que el grupo de invitados locales tenga acceso al registro de aplicaciones</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Evitar que el grupo de invitados locales tenga acceso al registro de seguridad</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Evitar que el grupo de invitados locales tenga acceso al registro del sistema</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Método de retención del registro de la aplicación</td><td>Según se necesite</td><td></td></tr>
<tr><td colspan="2">Método de retención del registro de seguridad</td><td>Según se necesite</td><td></td></tr>
<tr><td colspan="2">Método de retención del registro del sistema</td><td>Según se necesite</td><td></td></tr>
<tr><td colspan="2">Tamaño máximo del registro de la aplicación</td><td>32768 kilobytes</td><td></td></tr>
<tr><td colspan="2">Tamaño máximo del registro de seguridad</td><td>163840 kilobytes</td><td></td></tr>
<tr><td colspan="2">Tamaño máximo del registro del sistema</td><td>32768 kilobytes</td><td></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
13. Verifique los servicios del sistema en la directiva de grupo "CCN-STIC-570A ENS incremental Controladores de Dominio categoria media".		Seleccione el siguiente nodo. **"Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"** **Nota:** Dependiendo de los servicios que estén instalados en el equipo, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales (antivirus, etc.). En la siguiente tabla se muestran el nombre largo y el nombre corto para cada servicio. En la ventana del editor de administración de directivas de grupo sólo aparecerá uno de los dos: el nombre largo si el servicio está instalado en el sistema o el nombre corto si no lo está. Además, deberá tener en cuenta que los números existentes en algunos servicios son aleatorios y cambian en cada equipo.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado	
Administración de aplicaciones	AppMgmt	Manual	Configurado	
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado	
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado	
Administración remota de Windows (WS-Management)	WinRM	Automático	Configurado	
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado	
Administrador de conexiones de acceso remoto	RasMan	Manual	Configurado	
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado	

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK

Comprobación	OK/NOK	Cómo hacerlo		
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado	
Administrador de credenciales	VaultSvc	Manual	Configurado	
Administrador de cuentas de seguridad	SamSs	Automático	Configurado	
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado	
Administrador de sesión local	LSM	Automático	Configurado	
Administrador de usuarios	UserManager	Automático	Configurado	
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado	
Agente de conexión de red	NcbService	Manual	Configurado	
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado	
Agente de directiva IPsec	PolicyAgent	Manual	Configurado	
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado	
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado	
Aislamiento de claves CNG	KeyIso	Manual	Configurado	
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado	
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado	
Aplicación auxiliar IP	iphlpsvc	Automático	Configurado	
Aplicación del sistema COM+	COMSysApp	Manual	Configurado	
Archivos sin conexión	CscService	Deshabilitado	Configurado	
Asignador de detección de topologías de nivel de vínculo	lltdsvc	Manual	Configurado	
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Asistente para la conectividad de red	NcaSvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Audio de Windows	Audiosrv	Manual	Configurado	
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Deshabilitado	Configurado	
Ayudante especial de la consola de administración	sacsvr	Manual	Configurado	
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado	
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado	
CDPUserSvc	CDPUserSvc	Automático	Configurado	
Centro de distribución de claves Kerberos	Kdc	Automático	Configurado	
Cliente de directiva de grupo	gpsvc	Automático	Configurado	
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático	Configurado	
Cliente DHCP	Dhcp	Automático	Configurado	
Cliente DNS	Dnscache	Automático	Configurado	
Cola de impresión	Spooler	Automático	Configurado	
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Manual	Configurado	
Comprobador puntual	svsvc	Manual	Configurado	
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado	
Conexiones de red	Netman	Manual	Configurado	
Configuración automática de redes cableadas	dot3svc	Manual	Configurado	
Configuración de Escritorio remoto	SessionEnv	Manual	Configurado	
Conjunto resultante de proveedor de directivas	RSoPProv	Manual	Configurado	
Contenedor de Microsoft Passport	NgcCtnrSvc	Manual	Configurado	
Coordinador de transacciones distribuidas	MSDTC	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado	
DataCollectionPublishi	DcpSvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
ngService					
Datos de contactos		PimIndexMaintenanceSvc	Manual	Configurado	
Detección de hardware shell		ShellHWDetection	Deshabilitado	Configurado	
Detección de servicios interactivos		UI0Detect	Manual	Configurado	
Detección SSDP		SSDPSRV	Deshabilitado	Configurado	
Directiva de extracción de tarjetas inteligentes		SCPolicySvc	Manual	Configurado	
Disco virtual		vds	Manual	Configurado	
Dispositivo host de UPnP		upnphost	Manual	Configurado	
DLL de host del Contador de rendimiento		PerfHost	Manual	Configurado	
dmwappushsvc		dmwappushservice	Deshabilitado	Configurado	
Energía		Power	Automático	Configurado	
Enrutamiento y acceso remoto		RemoteAccess	Deshabilitado	Configurado	
Espacio de nombres DFS		Dfs	Automático	Configurado	
Estación de trabajo		LanmanWorkstation	Automático	Configurado	
Eventos de adquisición de imágenes estáticas		WiaRpc	Manual	Configurado	
Examinador de equipos		Browser	Deshabilitado	Configurado	
Experiencia de calidad de audio y vídeo de Windows (qWave)		QWAVE	Deshabilitado	Configurado	
Extensiones y notificaciones de impresora		PrintNotify	Manual	Configurado	
Firewall de Windows		MpsSvc	Automático	Configurado	
Hora de Windows		W32Time	Automático	Configurado	
Host de proveedor de detección de función		fdPHost	Deshabilitado	Configurado	
Host de sistema de diagnóstico		WdiSystemHost	Deshabilitado	Configurado	
Host del servicio de diagnóstico		WdiServiceHost	Deshabilitado	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Identidad de aplicación		AppIDSvc	Manual	Configurado	
Información de la aplicación		Appinfo	Manual	Configurado	
Iniciador de procesos		DcomLaunch	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
de servidor DCOM					
Inicio de sesión secundario		seclogon	Deshabilitado	Configurado	
Instalador de ActiveX (AxInstSV)		AxInstSV	Manual	Configurado	
Instalador de módulos de Windows		TrustedInstaller	Manual	Configurado	
Instantáneas de volumen		VSS	Manual	Configurado	
Instrumental de administración de Windows		Winmgmt	Automático	Configurado	
Interfaz de servicio invitado de Hyper-V		vmicguestinterface	Manual	Configurado	
KTMRM para DTC (Coordinador de transacciones distribuidas)		KtmRm	Manual	Configurado	
Llamada a procedimiento remoto (RPC)		RpcSs	Automático	Configurado	
Mensajería entre sitios		IsmServ	Automático	Configurado	
Microsoft App-V Client		AppVClient	Deshabilitado	Configurado	
Microsoft Passport		NgcSvc	Manual	Configurado	
Modo incrustado		embeddedmode	Manual	Configurado	
Módulos de creación de claves de IPsec para IKE y AuthIP		IKEEXT	Manual	Configurado	
Motor de filtrado de base		BFE	Automático	Configurado	
Net Logon		Netlogon	Automático	Configurado	
Optimizar unidades		defragsvc	Manual	Configurado	
Partida guardada en Xbox Live		XblGameSave	Deshabilitado	Configurado	
Plug and Play		PlugPlay	Manual	Configurado	
Preparación de aplicaciones		AppReadiness	Manual	Configurado	
Programador de tareas		Schedule	Automático	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Propagación de certificados		CertPropSvc	Manual	Configurado	
Protección de software		sppsvc	Automático	Configurado	
Protocolo de autenticación extensible		Eaphost	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Proveedor de instantáneas de software de Microsoft	swprv		Manual	Configurado	
Publicación de recurso de detección de función	FDResPub		Deshabilitado	Configurado	
Reconoc. ubicación de red	NlaSvc		Automático	Configurado	
Recopilador de eventos de Windows	Wecsvc		Manual	Configurado	
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService		Manual	Configurado	
Registro de eventos de Windows	EventLog		Automático	Configurado	
Registro remoto	RemoteRegistry		Automático	Configurado	
Registros y alertas de rendimiento	pla		Manual	Configurado	
Replicación de archivos	NtFrs		Deshabilitado	Configurado	
Replicación DFS	DFSR		Automático	Configurado	
Servicio Asistente para la compatibilidad de programas	PcaSvc		Automático	Configurado	
Servicio biométrico de Windows	WbioSrvc		Manual	Configurado	
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc		Manual	Configurado	
Servicio de administración de aplicaciones de empresa	EntAppSvc		Manual	Configurado	
Servicio de administración de radio	RmSvc		Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**		**Inicio**	**Permiso**	**OK/NOK**
Servicio de administrador de licencias de Windows	LicenseManager		Manual	Configurado	
Servicio de almacenamiento	StorSvc		Manual	Configurado	
Servicio de asociación de dispositivos	DeviceAssociationService		Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio de caché de fuentes de Windows	FontCache	Deshabilitado	Configurado		
Servicio de cierre de invitado de Hyper-V	vmicshutdown	Manual	Configurado		
Servicio de compatibilidad con Bluetooth	bthserv	Manual	Configurado		
Servicio de configuración de red	NetSetupSvc	Manual	Configurado		
Servicio de datos del sensor	SensorDataService	Manual	Configurado		
Servicio de detección automática de proxy web WinHTTP	WinHttpAutoProxySvc	Manual	Configurado		
Servicio de directivas de diagnóstico	DPS	Deshabilitado	Configurado		
Servicio de dispositivo de interfaz humana	hidserv	Manual	Configurado		
Servicio de distribución de clave de Microsoft	KdsSvc	Manual	Configurado		
Servicio de enrutador de AllJoyn	AJRouter	Deshabilitado	Configurado		
Servicio de enumeración de dispositivos de tarjeta inteligente	ScDeviceEnum	Manual	Configurado		
Servicio de geolocalización	lfsvc	Manual	Configurado		
Servicio de host HV	HvHost	Manual	Configurado		
Servicio de implementación de AppX (AppXSVC)	AppXSvc	Manual	Configurado		
Servicio de infraestructura de tareas en segundo plano	BrokerInfrastructure	Automático	Configurado		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**	
Servicio de inscripción de administración de dispositivos	DmEnrollmentSvc	Manual	Configurado		
Servicio de inspección de red de Windows Defender	WdNisSvc	Manual	Configurado		
Servicio de instalación de dispositivos	DeviceInstall	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado		
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado		
Servicio de licencia de cliente (ClipSVC)	ClipSVC	Manual	Configurado		
Servicio de lista de redes	netprofm	Manual	Configurado		
Servicio de notificación de eventos de sistema	SENS	Automático	Configurado		
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService	Deshabilitado	Configurado		
Servicio de perfil de usuario	ProfSvc	Automático	Configurado		
Servicio de plataforma de dispositivos conectados	CDPSvc	Automático	Configurado		
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Manual	Configurado		
Servicio de puerta de enlace de nivel de aplicación	ALG	Manual	Configurado		
Servicio de registro de acceso de usuarios	UALSVC	Automático	Configurado		
Servicio de repositorio de estado	StateRepository	Manual	Configurado		
Servicio de sensores	SensorService	Manual	Configurado		
Servicio de servidor proxy KDC (KPS)	KPSSVC	Manual	Configurado		
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**	
Servicio de supervisión de licencias de Windows	WLMS	Automático	Configurado		
Servicio de supervisión de sensores	SensrSvc	Manual	Configurado		
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Manual	Configurado		
Servicio de uso	DsSvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
compartido de datos					
Servicio de uso compartido de puertos Net.Tcp		NetTcpPortSharing	Deshabilitado	Configurado	
Servicio de usuario de notificaciones de inserción de Windows		WpnUserService	Manual	Configurado	
Servicio de virtualización de Escritorio remoto de Hyper-V		vmicrdv	Manual	Configurado	
Servicio de virtualización de la experiencia de usuario		UevAgentService	Deshabilitado	Configurado	
Servicio de Windows Defender		WinDefend	Automático	Configurado	
Servicio de Windows Insider		wisvc	Manual	Configurado	
Servicio de zona con cobertura inalámbrica móvil de Windows		icssvc	Deshabilitado	Configurado	
Servicio del iniciador iSCSI de Microsoft		MSiSCSI	Manual	Configurado	
Servicio del sistema de notificaciones de inserción de Windows		WpnService	Automático	Configurado	
Servicio enumerador de dispositivos portátiles		WPDBusEnum	Manual	Configurado	
Servicio FrameServer de la Cámara de Windows		FrameServer	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio host de proveedor de cifrado de Windows		WEPHOSTSVC	Manual	Configurado	
Servicio Informe de errores de Windows		WerSvc	Deshabilitado	Configurado	
Servicio Interfaz de almacenamiento en red		nsi	Automático	Configurado	
Servicio PowerShell Direct de Hyper-V		vmicvmsession	Manual	Configurado	
Servicio Recopilador estándar del		diagnosticshub.standardcollector.service	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
concentrador de diagnósticos de Microsoft (R)				
Servicio telefónico	PhoneSvc	Manual	Configurado	
Servicios de cifrado	CryptSvc	Automático	Configurado	
Servicios de dominio de Active Directory	NTDS	Automático	Configurado	
Servicios de Escritorio remoto	TermService	Manual	Configurado	
Servicios web de Active Directory	ADWS	Automático	Configurado	
Servidor	LanmanServer	Automático	Configurado	
Servidor de roles de DS	DsRoleSvc	Manual	Configurado	
Servidor del modelo de datos del mosaico	tiledatamodelsvc	Automático	Configurado	
Servidor DNS	DNS	Automático	Configurado	
Sincronizar host	OneSyncSvc	Automático	Configurado	
Sistema de cifrado de archivos (EFS)	EFS	Manual	Configurado	
Sistema de eventos COM+	EventSystem	Automático	Configurado	
SMP de Espacios de almacenamiento de Microsoft	smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado	
Superfetch	SysMain	Manual	Configurado	
Tarjeta inteligente	SCardSvr	Deshabilitado	Configurado	
Telefonía	TapiSrv	Deshabilitado	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Telemetría y experiencias del usuario conectado	DiagTrack	Automático	Configurado	
Temas	Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)	RpcLocator	Manual	Configurado	
WalletService	WalletService	Manual	Configurado	
Windows Driver Foundation - User-mode Driver Framework	wudfsvc	Manual	Configurado	
Windows Installer	msiserver	Manual	Configurado	
Windows Search	WSearch	Deshabilitado	Configurado	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="4">Cómo hacerlo</th></tr>
<tr><td colspan="2">Windows Update</td><td>wuauserv</td><td>Manual</td><td>Configurado</td><td></td></tr>
<tr><td rowspan="3">14. Verifique los permisos de valores de registro de la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.</td><td></td><td colspan="4">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro”

Nota: Para verificar los permisos de la entrada de registro, deberá pulsar doble clic sobre la entrada “MACHINES → SOFTWARE → Microsoft → Windows → CurrentVersion → Installer” y pulsar sobre el botón "Modificar seguridad...".

Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".</td></tr>
<tr><td colspan="2">Directiva</td><td colspan="2">Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer</td><td colspan="2">Administradores: Control Total
SYSTEM: Control Total
Usuarios: Leer</td><td></td></tr>
<tr><td>15. Verifique los valores del sistema de archivos de la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.</td><td></td><td colspan="4">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de Archivos”

Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción “Propiedades” del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...".

Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\Registration	Administrador	Control total	
	System	Control total	
	Usuario	Leer y ejecutar	
%SystemRoot%\repair	Administrador	Control total	
	System	Control total	
%SystemRoot%\security	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\cacls.exe	Administrador	Control total	
	System	Control total	
SystemRoot%\system32\clip.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\ras	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\rasadhlp.dll	Administrador	Control total	
%SystemRoot%\system32\rasauto.dll	Administrador	Control total	
%SystemRoot%\system32\rasautou.exe	Administrador	Control total	
%SystemRoot%\system32\raschap.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrnm.h	Administrador	Control total	
%SystemRoot%\system32\rasctrs.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrs.ini	Administrador	Control total	
%SystemRoot%\system32\rasdial.exe	Administrador	Control total	
%SystemRoot%\system32\rasmans.dll	Administrador	Control total	
%SystemRoot%\system32\rasmontr.dll	Administrador	Control total	
%SystemRoot%\system32\rasphone.exe	Administrador	Control total	
%SystemRoot%\system32\rasppp.dll	Administrador	Control total	
%SystemRoot%\system32\rastapi.dll	Administrador	Control total	

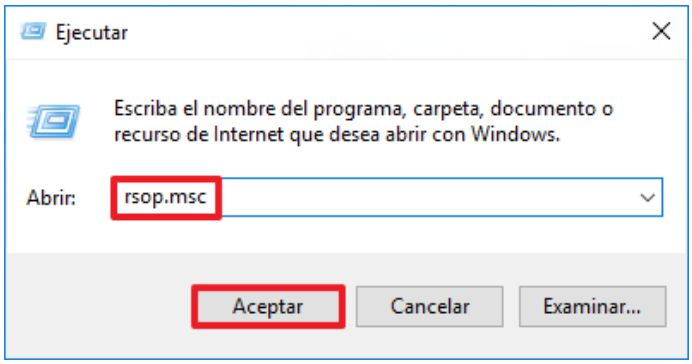
Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\system32\rastls.dll	Administrador	Control total	
%SystemRoot%\system32\runonce.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\secedit.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\telnet.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tftp.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tracert.exe	Administrador	Control total	
	System	Control total	

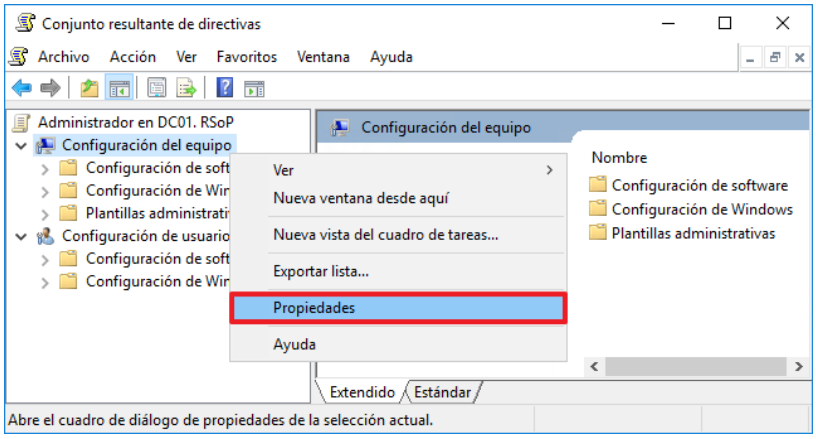
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td rowspan="3">16. Verifique que está bloqueada la ejecución del Almacén digital en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Administración de derechos digitales de Windows Media”</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Impedir el acceso a internet de Windows Media DRM</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td></td></tr>
<tr><td rowspan="3">17. Verifique que está bloqueada la ejecución del Almacén digital en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Almacén Digital”</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>No permitir que se ejecute el Almacén digital</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td></td></tr>
</table>

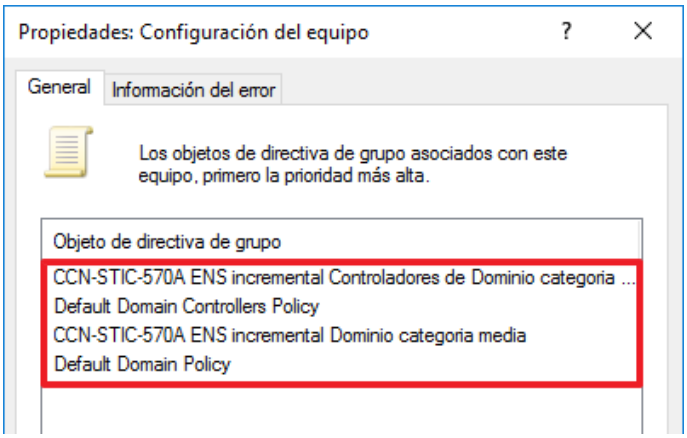
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>18. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Biometría”</td></tr>
<tr><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Permitir el uso de biometría</td><td>Habilitada</td><td></td></tr>
<tr><td>Permitir que los usuarios de dominio inicien sesión mediante biometría</td><td>Habilitada</td><td></td></tr>
<tr><td>Permitir que los usuarios inicien sesión mediante biometría</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td>19. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Directivas de reproducción automática”</td></tr>
<tr><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Desactivar reproducción automática</td><td>Habilitada</td><td></td></tr>
<tr><td>Establecer el comportamiento predeterminado para ejecución automática.</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td rowspan="4">20. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.</td><td></td><td colspan="2">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Informe de errores de Windows”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Deshabilitar el informe de errores de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">No enviar datos adicionales</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="4">21. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.</td><td></td><td colspan="2">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Opciones de inicio de sesión de Windows”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Informar cuando el servidor de inicio de sesión no está disponible durante el inicio de sesión del usuario</td><td>Habilitada</td><td></td></tr>
</table>

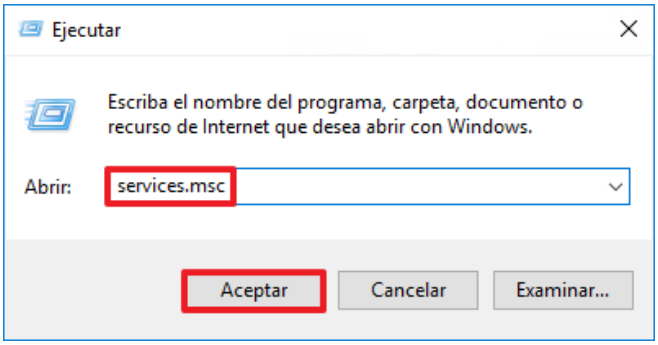
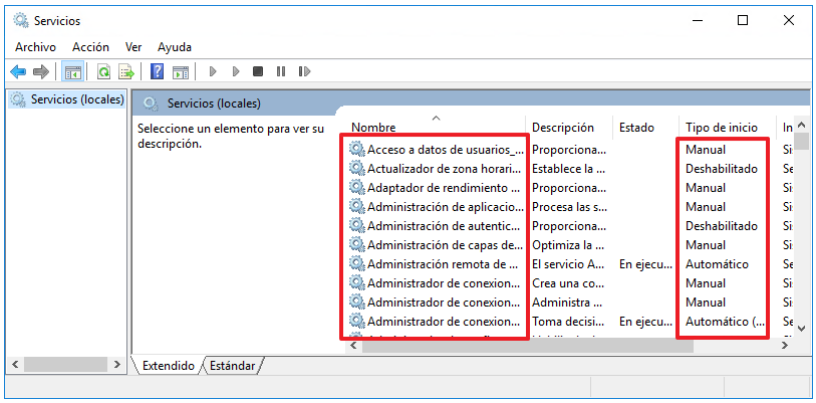
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>22. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Shell remoto de Windows”
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Permitir acceso a Shell remoto</td><td>Deshabilitada</td><td></td></tr>
</table></td></tr>
<tr><td>23. Verifique configuración de la comunicación de Internet en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Desactivar informe de errores de reconocimiento de escritura a mano</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el Programa para la mejora de la experiencia del usuario de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar los vínculos “Events.asp” del Visor de eventos</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el contenido “¿Sabía que…?” del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la búsqueda en Microsoft Knowledge Base del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el informe de errores de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la actualización de archivos de contenido del Asistente para búsqueda</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Desactivar el acceso a la Tienda</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la tarea de imágenes “Pedir copias fotográficas”</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td rowspan="2">24. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Sistema → Net Logon”</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Permitir algoritmos de criptografía compatibles con Windows NT 4.0</td><td>Deshabilitada</td><td></td></tr>
</table></td></tr>
<tr><td>25. Verifique que el equipo ha recibido las directivas de grupo CC-STIC-570A ENS incremental Dominio categoria media y CCN-STIC-570A ENS incremental Controladores de Dominio categoria media</td><td></td><td>Ejecute la consola de administración "Conjunto resultante de directivas" (el sistema solicitará elevación de privilegios):
“Tecla Windows+R → rsop.msc”
El Control de cuentas de usuario solicitará elevación de privilegios. Pulse “Sí” para continuar.
 
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>
Seleccione en ella la rama "Configuración del equipo", márquela con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la figura:


En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", resaltada en la siguiente figura:


Verifique que en dicha sección aparecen listados, y por ese orden, los objetos de directiva de grupo que se indican en la siguiente tabla:
<table>
<tr><th>Objeto de directiva de grupo</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-570A ENS incremental Controladores de Dominio categoria media</td><td></td></tr>
<tr><td>Default Domain Controllers Policy</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS incremental Dominio categoria media</td><td></td></tr>
<tr><td>Default Domain Policy</td><td></td></tr>
</table>
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
26. Verifique que los servicios del sistema están correctamente configurados		Usando la consola de servicios (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → services.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" para continuar.  Verifique que el tipo de inicio de los servicios que aparecen en el sistema y en la siguiente tabla coinciden:  **Nota:** Dependiendo del equipo, es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales (antivirus, etc.).

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado	
Administración de aplicaciones	AppMgmt	Manual	Configurado	
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado	
Administración remota de Windows (WS-Management)	WinRM	Automático	Configurado	
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado	
Administrador de conexiones de acceso remoto	RasMan	Manual	Configurado	
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado	
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado	
Administrador de credenciales	VaultSvc	Manual	Configurado	
Administrador de cuentas de seguridad	SamSs	Automático	Configurado	
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado	
Administrador de sesión local	LSM	Automático	Configurado	
Administrador de usuarios	UserManager	Automático	Configurado	
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado	
Agente de conexión de red	NcbService	Manual	Configurado	
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado	
Agente de directiva IPsec	PolicyAgent	Manual	Configurado	
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado	
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**

Comprobación	OK/NOK	Cómo hacerlo		
Aislamiento de claves CNG	KeyIso	Manual	Configurado	
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado	
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado	
Aplicación auxiliar IP	iphlpsvc	Automático	Configurado	
Aplicación del sistema COM+	COMSysApp	Manual	Configurado	
Archivos sin conexión	CscService	Deshabilitado	Configurado	
Asignador de detección de topologías de nivel de vínculo	lltdsvc	Manual	Configurado	
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado	
Asistente para la conectividad de red	NcaSvc	Manual	Configurado	
Audio de Windows	Audiosrv	Manual	Configurado	
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Deshabilitado	Configurado	
Ayudante especial de la consola de administración	sacsvr	Manual	Configurado	
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado	
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado	
CDPUserSvc	CDPUserSvc	Automático	Configurado	
Centro de distribución de claves Kerberos	Kdc	Automático	Configurado	
Cliente de directiva de grupo	gpsvc	Automático	Configurado	
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático	Configurado	
Cliente DHCP	Dhcp	Automático	Configurado	
Cliente DNS	Dnscache	Automático	Configurado	
Cola de impresión	Spooler	Automático	Configurado	
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Manual	Configurado	
Comprobador puntual	svsvc	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Conexiones de red	Netman	Manual	Configurado	
Configuración automática de redes cableadas	dot3svc	Manual	Configurado	
Configuración de Escritorio remoto	SessionEnv	Manual	Configurado	
Conjunto resultante de proveedor de directivas	RSoPProv	Manual	Configurado	
Contenedor de Microsoft Passport	NgcCtnrSvc	Manual	Configurado	
Coordinador de transacciones distribuidas	MSDTC	Automático	Configurado	
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado	
DataCollectionPublishingService	DcpSvc	Manual	Configurado	
Datos de contactos	PimIndexMaintenanceSvc	Manual	Configurado	
Detección de hardware shell	ShellHWDetection	Deshabilitado	Configurado	
Detección de servicios interactivos	UI0Detect	Manual	Configurado	
Detección SSDP	SSDPSRV	Deshabilitado	Configurado	
Directiva de extracción de tarjetas inteligentes	SCPolicySvc	Manual	Configurado	
Disco virtual	vds	Manual	Configurado	
Dispositivo host de UPnP	upnphost	Manual	Configurado	
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado	
dmwappushsvc	dmwappushservice	Deshabilitado	Configurado	
Energía	Power	Automático	Configurado	
Enrutamiento y acceso remoto	RemoteAccess	Deshabilitado	Configurado	
Espacio de nombres DFS	Dfs	Automático	Configurado	
Estación de trabajo	LanmanWorkstation	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Eventos de adquisición de imágenes estáticas	WiaRpc	Manual	Configurado	
Examinador de equipos	Browser	Deshabilitado	Configurado	
Experiencia de calidad	QWAVE	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
de audio y vídeo de Windows (qWave)					
Extensiones y notificaciones de impresora	PrintNotify	Manual	Configurado		
Firewall de Windows	MpsSvc	Automático	Configurado		
Hora de Windows	W32Time	Automático	Configurado		
Host de proveedor de detección de función	fdPHost	Deshabilitado	Configurado		
Host de sistema de diagnóstico	WdiSystemHost	Deshabilitado	Configurado		
Host del servicio de diagnóstico	WdiServiceHost	Deshabilitado	Configurado		
Identidad de aplicación	AppIDSvc	Manual	Configurado		
Información de la aplicación	Appinfo	Manual	Configurado		
Iniciador de procesos de servidor DCOM	DcomLaunch	Automático	Configurado		
Inicio de sesión secundario	seclogon	Deshabilitado	Configurado		
Instalador de ActiveX (AxInstSV)	AxInstSV	Manual	Configurado		
Instalador de módulos de Windows	TrustedInstaller	Manual	Configurado		
Instantáneas de volumen	VSS	Manual	Configurado		
Instrumental de administración de Windows	Winmgmt	Automático	Configurado		
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado		
KTMRM para DTC (Coordinador de transacciones distribuidas)	KtmRm	Manual	Configurado		
Llamada a procedimiento remoto (RPC)	RpcSs	Automático	Configurado		
Mensajería entre sitios	IsmServ	Automático	Configurado		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**	
Microsoft App-V Client	AppVClient	Deshabilitado	Configurado		
Microsoft Passport	NgcSvc	Manual	Configurado		
Modo incrustado	embeddedmode	Manual	Configurado		
Módulos de creación de claves de IPsec para	IKEEXT	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
IKE y AuthIP					
Motor de filtrado de base	BFE		Automático	Configurado	
Net Logon	Netlogon		Automático	Configurado	
Optimizar unidades	defragsvc		Manual	Configurado	
Partida guardada en Xbox Live	XblGameSave		Deshabilitado	Configurado	
Plug and Play	PlugPlay		Manual	Configurado	
Preparación de aplicaciones	AppReadiness		Manual	Configurado	
Programador de tareas	Schedule		Automático	Configurado	
Propagación de certificados	CertPropSvc		Manual	Configurado	
Protección de software	sppsvc		Automático	Configurado	
Protocolo de autenticación extensible	Eaphost		Manual	Configurado	
Proveedor de instantáneas de software de Microsoft	swprv		Manual	Configurado	
Publicación de recurso de detección de función	FDResPub		Deshabilitado	Configurado	
Reconoc. ubicación de red	NlaSvc		Automático	Configurado	
Recopilador de eventos de Windows	Wecsvc		Manual	Configurado	
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService		Manual	Configurado	
Registro de eventos de Windows	EventLog		Automático	Configurado	
Registro remoto	RemoteRegistry		Automático	Configurado	
Registros y alertas de rendimiento	pla		Manual	Configurado	
Replicación de archivos	NtFrs		Deshabilitado	Configurado	
Replicación DFS	DFSR		Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**		**Inicio**	**Permiso**	**OK/NOK**
Servicio Asistente para la compatibilidad de programas	PcaSvc		Automático	Configurado	
Servicio biométrico de Windows	WbioSrvc		Manual	Configurado	
Servicio de	UsoSvc		Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
actualizaciones Orchestrator para Windows Update					
Servicio de administración de aplicaciones de empresa		EntAppSvc	Manual	Configurado	
Servicio de administración de radio		RmSvc	Manual	Configurado	
Servicio de administrador de licencias de Windows		LicenseManager	Manual	Configurado	
Servicio de almacenamiento		StorSvc	Manual	Configurado	
Servicio de asociación de dispositivos		DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows		FontCache	Deshabilitado	Configurado	
Servicio de cierre de invitado de Hyper-V		vmicshutdown	Manual	Configurado	
Servicio de compatibilidad con Bluetooth		bthserv	Manual	Configurado	
Servicio de configuración de red		NetSetupSvc	Manual	Configurado	
Servicio de datos del sensor		SensorDataService	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP		WinHttpAutoProxySvc	Manual	Configurado	
Servicio de directivas de diagnóstico		DPS	Deshabilitado	Configurado	
Servicio de dispositivo de interfaz humana		hidserv	Manual	Configurado	
Servicio de distribución de clave de Microsoft		KdsSvc	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de enrutador de AllJoyn		AJRouter	Deshabilitado	Configurado	
Servicio de enumeración de dispositivos de tarjeta inteligente		ScDeviceEnum	Manual	Configurado	
Servicio de		lfsvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
geolocalización					
Servicio de host HV		HvHost	Manual	Configurado	
Servicio de implementación de AppX (AppXSVC)		AppXSvc	Manual	Configurado	
Servicio de infraestructura de tareas en segundo plano		BrokerInfrastructure	Automático	Configurado	
Servicio de inscripción de administración de dispositivos		DmEnrollmentSvc	Manual	Configurado	
Servicio de inspección de red de Windows Defender		WdNisSvc	Manual	Configurado	
Servicio de instalación de dispositivos		DeviceInstall	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V		vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V		vmicheartbeat	Manual	Configurado	
Servicio de licencia de cliente (ClipSVC)		ClipSVC	Manual	Configurado	
Servicio de lista de redes		netprofm	Manual	Configurado	
Servicio de notificación de eventos de sistema		SENS	Automático	Configurado	
Servicio de Panel de escritura a mano y teclado táctil		TabletInputService	Deshabilitado	Configurado	
Servicio de perfil de usuario		ProfSvc	Automático	Configurado	
Servicio de plataforma de dispositivos conectados		CDPSvc	Automático	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de protocolo de túnel de sockets seguros		SstpSvc	Manual	Configurado	
Servicio de puerta de enlace de nivel de aplicación		ALG	Manual	Configurado	
Servicio de registro de acceso de usuarios		UALSVC	Automático	Configurado	
Servicio de repositorio		StateRepository	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
de estado					
Servicio de sensores		SensorService	Manual	Configurado	
Servicio de servidor proxy KDC (KPS)		KPSSVC	Manual	Configurado	
Servicio de sincronización de hora de Hyper-V		vmictimesync	Manual	Configurado	
Servicio de supervisión de licencias de Windows		WLMS	Automático	Configurado	
Servicio de supervisión de sensores		SensrSvc	Manual	Configurado	
Servicio de transferencia inteligente en segundo plano (BITS)		BITS	Manual	Configurado	
Servicio de uso compartido de datos		DsSvc	Manual	Configurado	
Servicio de uso compartido de puertos Net.Tcp		NetTcpPortSharing	Deshabilitado	Configurado	
Servicio de usuario de notificaciones de inserción de Windows		WpnUserService	Manual	Configurado	
Servicio de virtualización de Escritorio remoto de Hyper-V		vmicrdv	Manual	Configurado	
Servicio de virtualización de la experiencia de usuario		UevAgentService	Deshabilitado	Configurado	
Servicio de Windows Defender		WinDefend	Automático	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de Windows Insider		wisvc	Manual	Configurado	
Servicio de zona con cobertura inalámbrica móvil de Windows		icssvc	Deshabilitado	Configurado	
Servicio del iniciador iSCSI de Microsoft		MSiSCSI	Manual	Configurado	
Servicio del sistema de notificaciones de inserción de Windows		WpnService	Automático	Configurado	
Servicio enumerador		WPDBusEnum	Manual	Configurado	

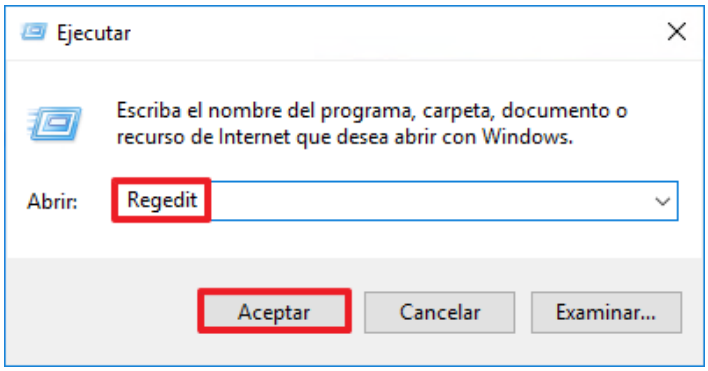
Comprobación	OK/NOK	Cómo hacerlo			
de dispositivos portátiles					
Servicio FrameServer de la Cámara de Windows		FrameServer	Manual	Configurado	
Servicio host de proveedor de cifrado de Windows		WEPHOSTSVC	Manual	Configurado	
Servicio Informe de errores de Windows		WerSvc	Deshabilitado	Configurado	
Servicio Interfaz de almacenamiento en red		nsi	Automático	Configurado	
Servicio PowerShell Direct de Hyper-V		vmicvmsession	Manual	Configurado	
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)		diagnosticshub.standardcollector.service	Manual	Configurado	
Servicio telefónico		PhoneSvc	Manual	Configurado	
Servicios de cifrado		CryptSvc	Automático	Configurado	
Servicios de dominio de Active Directory		NTDS	Automático	Configurado	
Servicios de Escritorio remoto		TermService	Manual	Configurado	
Servicios web de Active Directory		ADWS	Automático	Configurado	
Servidor		LanmanServer	Automático	Configurado	
Servidor de roles de DS		DsRoleSvc	Manual	Configurado	
Servidor del modelo de datos del mosaico		tiledatamodelsvc	Automático	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servidor DNS		DNS	Automático	Configurado	
Sincronizar host		OneSyncSvc	Automático	Configurado	
Sistema de cifrado de archivos (EFS)		EFS	Manual	Configurado	
Sistema de eventos COM+		EventSystem	Automático	Configurado	
SMP de Espacios de almacenamiento de Microsoft		smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V		vmicvss	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Superfetch		SysMain	Manual	Configurado	
Tarjeta inteligente		SCardSvr	Deshabilitado	Configurado	
Telefonía		TapiSrv	Deshabilitado	Configurado	
Telemetría y experiencias del usuario conectado		DiagTrack	Automático	Configurado	
Temas		Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)		RpcLocator	Manual	Configurado	
WalletService		WalletService	Manual	Configurado	
Windows Driver Foundation - User-mode Driver Framework		wudfsvc	Manual	Configurado	
Windows Installer		msiserver	Manual	Configurado	
Windows Search		WSearch	Deshabilitado	Configurado	
Windows Update		wuauserv	Manual	Configurado	
27. Verifique que se han asignado los permisos correctos en el sistema de archivos		Utilizando el Explorador de Windows: **"Windows+R → Explorer"** En caso de no saber dónde apunta cada una de las rutas abreviadas que se especifica, ejecute Explorer <<ruta>> donde <<ruta>> se sustituirá por la ruta abreviada.			
		Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, marcándolo con el botón derecho y eligiendo la opción "Propiedades" del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá situarse en la pestaña "Seguridad". En la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios. Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados.			

Comprobación	OK/NOK	Cómo hacerlo

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\Registration	Administrador	Control total	
	System	Control total	
	Usuario	Leer y ejecutar	
%SystemRoot%\repair	Administrador	Control total	
	System	Control total	
%SystemRoot%\security	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\cacls.exe	Administrador	Control total	
	System	Control total	
SystemRoot%\system32\clip.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\ras	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\rasadhlp.dll	Administrador	Control total	
%SystemRoot%\system32\rasauto.dll	Administrador	Control total	
%SystemRoot%\system32\rasautou.exe	Administrador	Control total	
%SystemRoot%\system32\raschap.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrnm.h	Administrador	Control total	
%SystemRoot%\system32\rasctrs.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrs.ini	Administrador	Control total	
%SystemRoot%\system32\rasdial.exe	Administrador	Control total	
%SystemRoot%\system32\rasmans.dll	Administrador	Control total	
%SystemRoot%\system32\rasmontr.dll	Administrador	Control total	
%SystemRoot%\system32\rasphone.exe	Administrador	Control total	
%SystemRoot%\system32\rasppp.dll	Administrador	Control total	
%SystemRoot%\system32\rastapi.dll	Administrador	Control total	
%SystemRoot%\system32\rastls.dll	Administrador	Control total	
%SystemRoot%\system32\runonce.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\secedit.exe	Administrador	Control total	
	System	Control total	

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\system32\telnet.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tftp.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tracert.exe	Administrador	Control total	
	System	Control total	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>28. Verifique los valores del Registro.</td><td></td><td>Compruebe los valores del registro definidos en los Controladores de Dominio que pertenezcan al grupo categorizado como categoría media siguiendo los criterios del ENS, mediante el uso del “Editor del Registro”.
“Windows+R → Regedit”
El Control de cuentas de usuario solicitará elevación de privilegios. Pulse “Sí” para continuar.
 

<table>
<tr><th>Valor del registro</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod</td><td>0</td><td></td></tr>
<tr><td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun</td><td>255</td><td></td></tr>
<tr><td>HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation</td><td>1</td><td></td></tr>
<tr><td>HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode</td><td>1</td><td></td></tr>
<tr><td>HKLM\System\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta</td><td>10</td><td></td></tr>
<tr><td>HKLM\System\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog</td><td>1</td><td></td></tr>
<tr><td>HKLM\System\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog</td><td>20000</td><td></td></tr>
</table></td></tr>
</table>

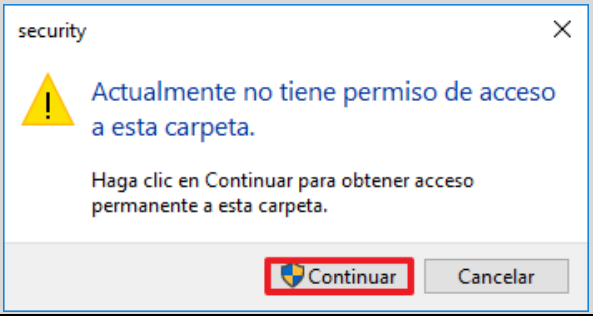
Comprobación	OK/NOK	Cómo hacerlo		
		Valor del registro	Valor	OK/NOK
		HKLM\System\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog	20	
		HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel	90	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect	0	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime	300000	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery	0	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect	1	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions	2	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions	3	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TCPMaxPortsExhausted	5	

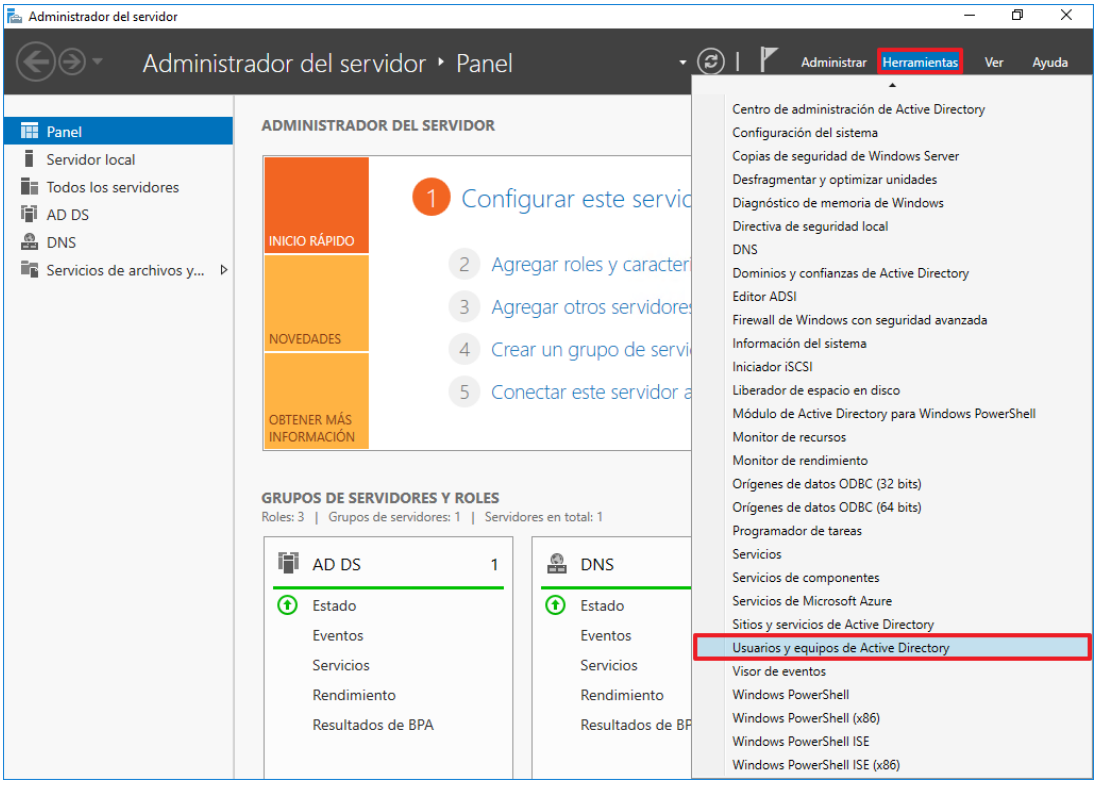
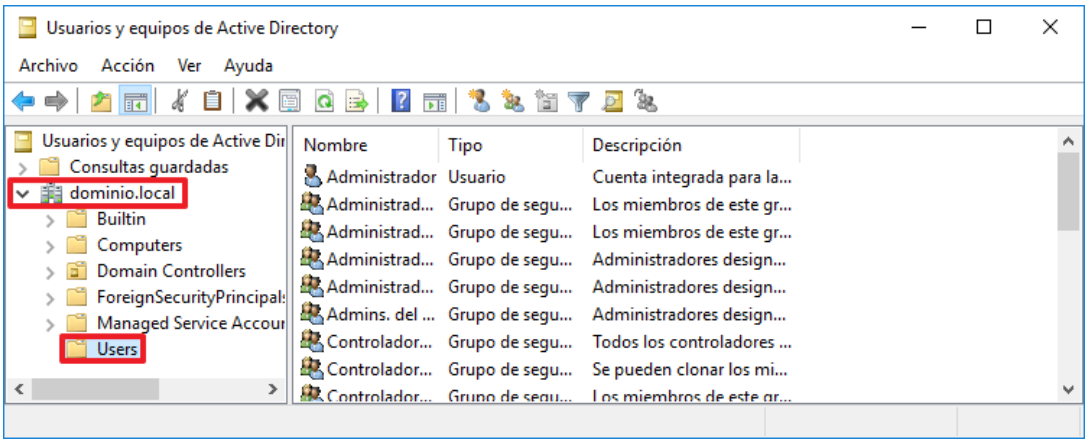
ANEXO A.3.3. GUÍA PASO A PASO SERVIDOR MIEMBRO QUE LE SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

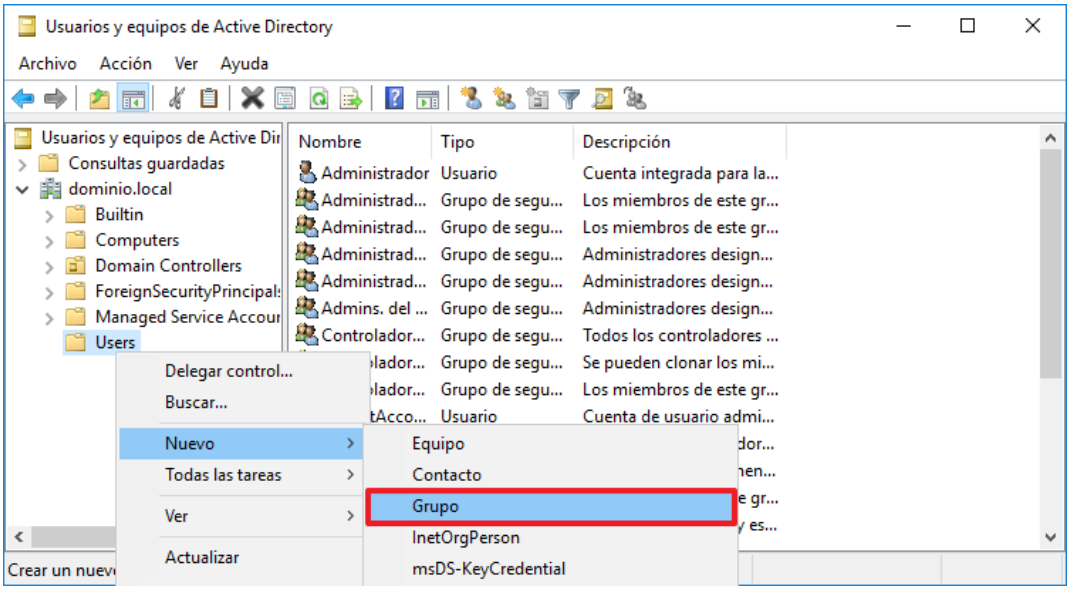
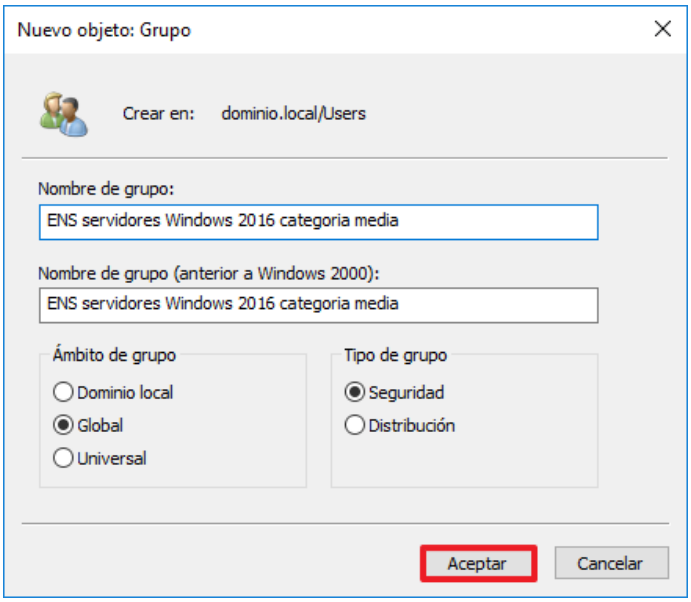
1. PREPARACIÓN DE DOMINIO

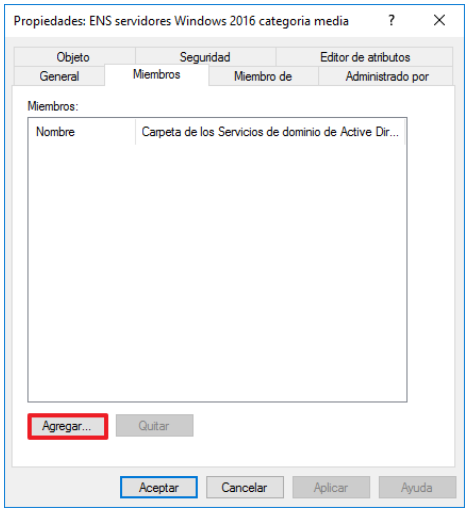
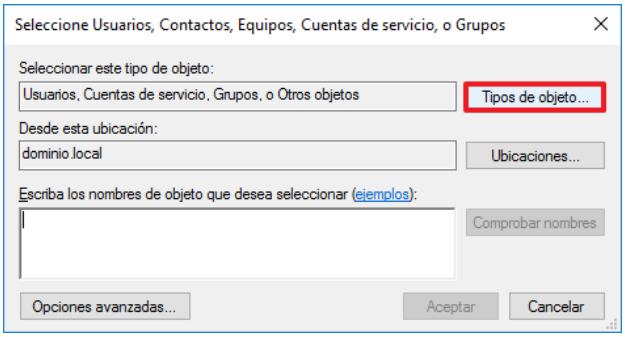
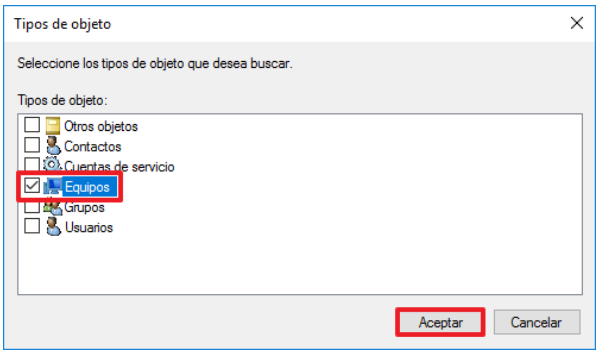
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se realizará la implementación de las plantillas de seguridad. Solo es necesario realizar este procedimiento una vez.

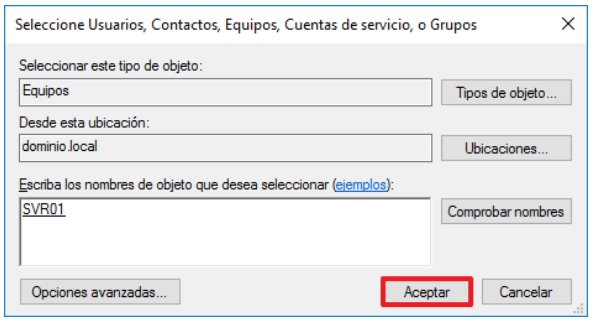
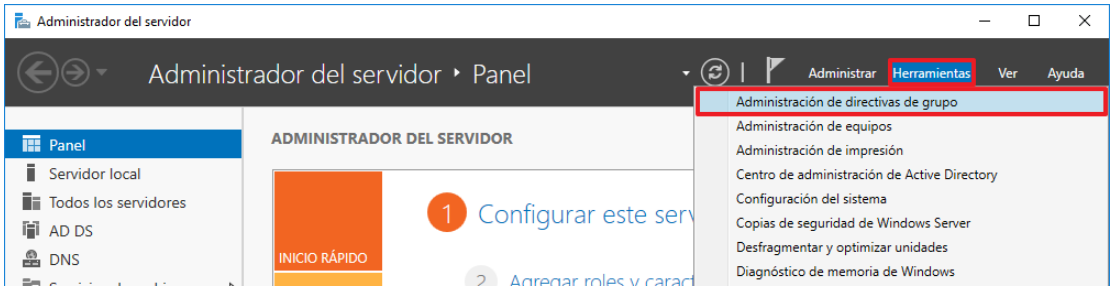
Nota: Esta guía asume que a los servidores controladores del dominio al que va a pertenecer el equipo cliente que está asegurando, se les ha aplicado la configuración descrita en el apartado "ANEXO A.3.1 GUÍA PASO A PASO CONTROLADOR DE DOMINIO QUE LE SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS" de la presente. Si no es así, aplique las configuraciones correspondientes al controlador de dominio, antes de continuar con la aplicación de ésta.

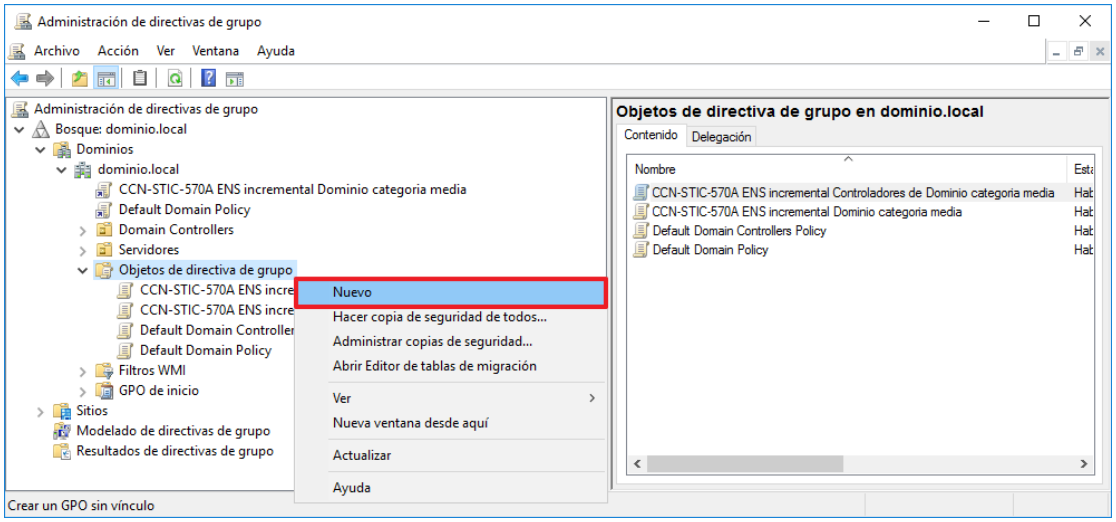
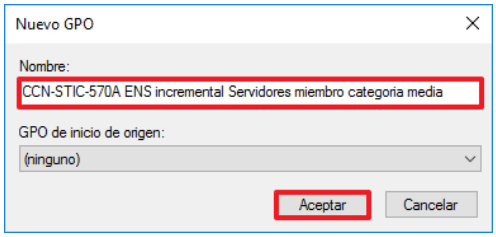
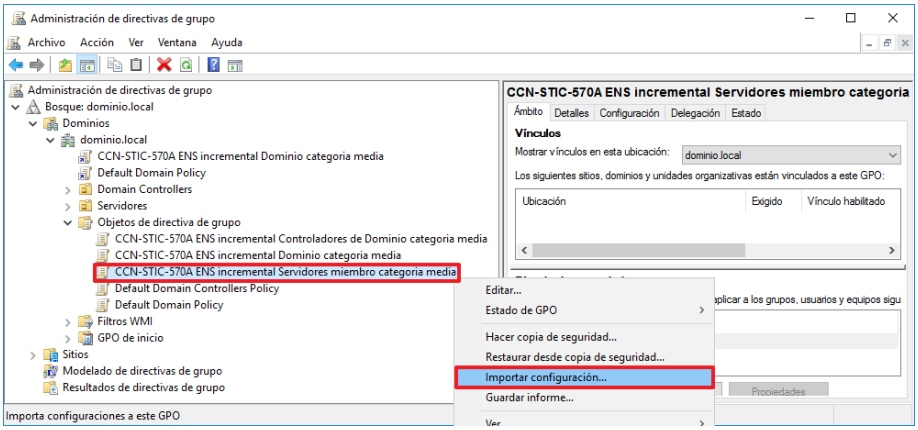
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Cree el directorio "Scripts" en la unidad C:\.
4.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts". **Nota:** Los recursos asociados a esta guía se encuentran en el directorio "Scripts-570A".
5.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio "C:\Scripts" del controlador de dominio: – CCN-STIC-570A ENS incremental DC categoria media (directorio) – CCN-STIC-570A ENS servidores categoria media (directorio) – CCN-STIC-570A ENS incremental DC categoria media.inf – CCN-STIC-570A ENS incremental dominio categoria media.inf – CCN-STIC-570A ENS Incremental servidores categoria media.inf
6.	Copie el fichero "CCN-STIC-570A ENS incremental servidores categoria media.inf", al directorio "%SYSTEMROOT%\Security\Templates" del Controlador de Dominio. **Nota:** Según la configuración de seguridad de UAC, el sistema podría solicitar la elevación de privilegios, en este caso, pulse "Continuar". 

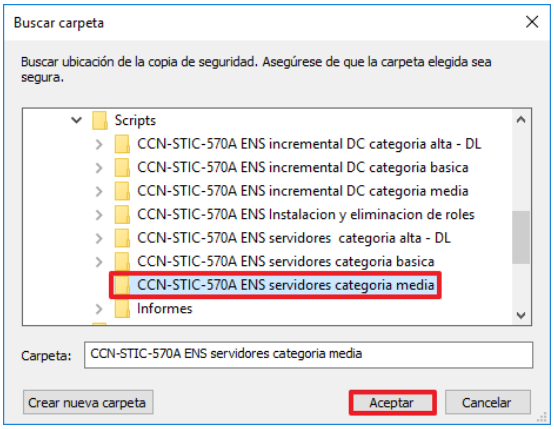
Paso	Descripción
7.	Inicie la herramienta de usuarios y equipos del Directorio Activo. Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Usuarios y equipos de Active Directory"** 
8.	Despliegue el dominio y vaya a la carpeta "Users". 

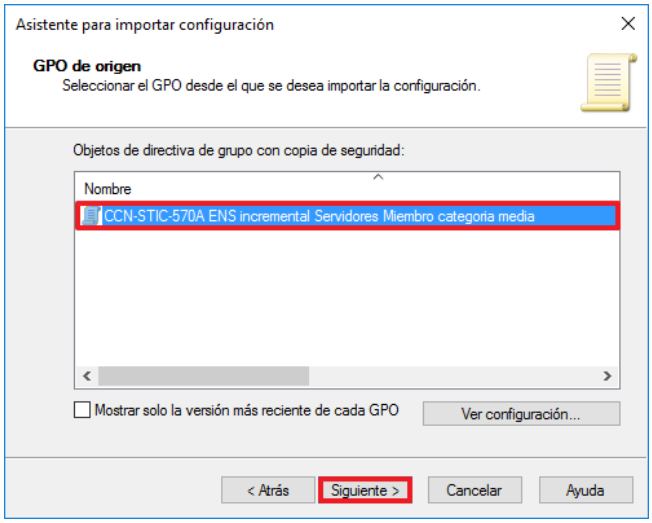
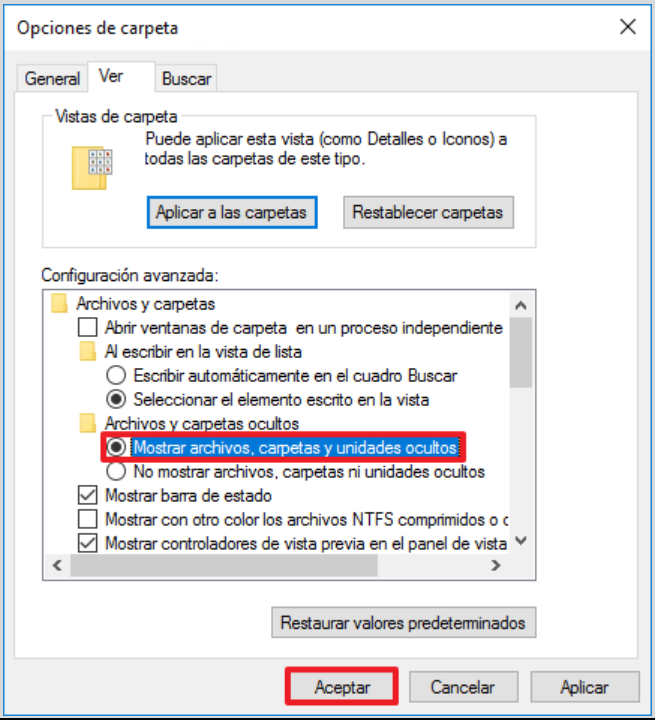
Paso	Descripción
9.	Pulse con el botón derecho sobre dicha carpeta y seleccione la opción **"Nuevo"→"Grupo".** 
10.	Introduzca como nombre "ENS servidores Windows 2016 categorIa media". Deje el resto de opciones como aparecen por defecto y pulse el botón "Aceptar". Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre servidores miembros del dominio a este grupo creado. 
11.	Abra el nuevo grupo creado pulsando doble clic sobre él y vaya a la pestaña "Miembros".

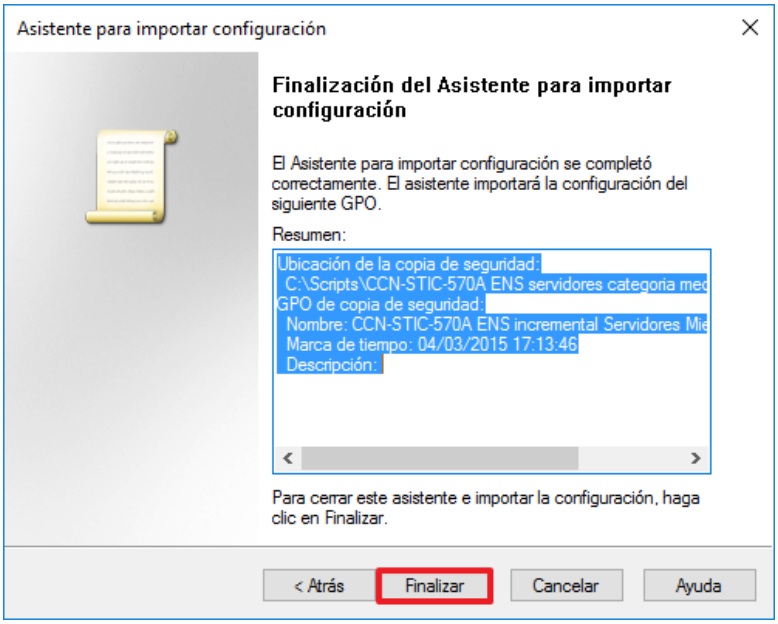
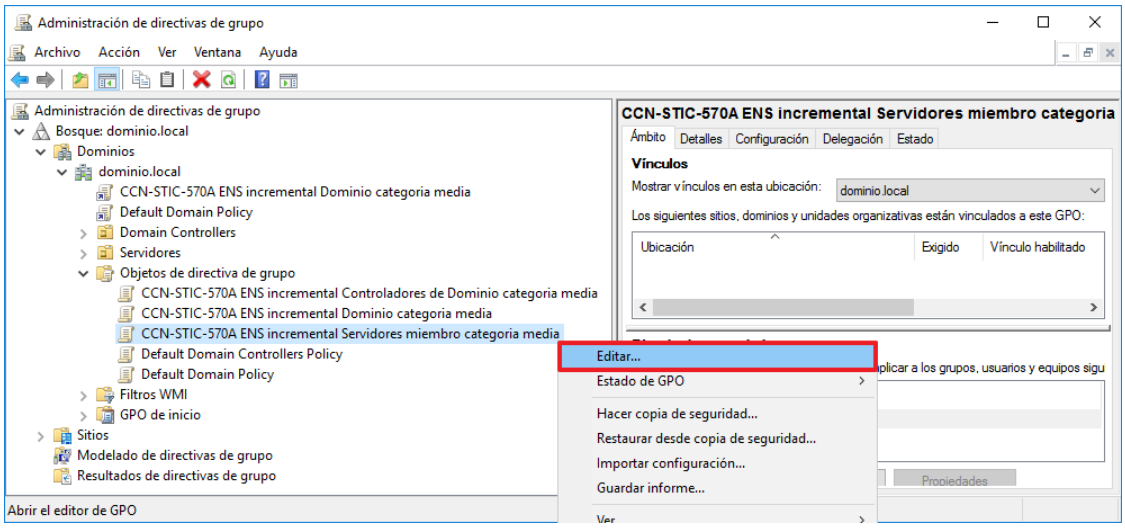
Paso	Descripción
12.	Pulse el botón “Agregar…”. 
13.	Pulse el botón “Tipos de objeto…”. 
14.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 

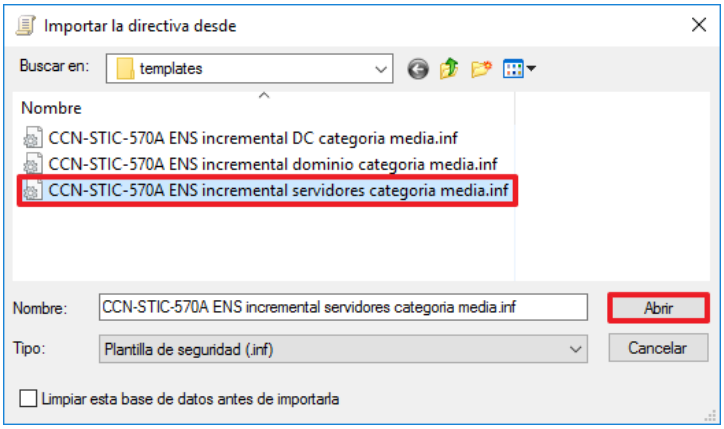
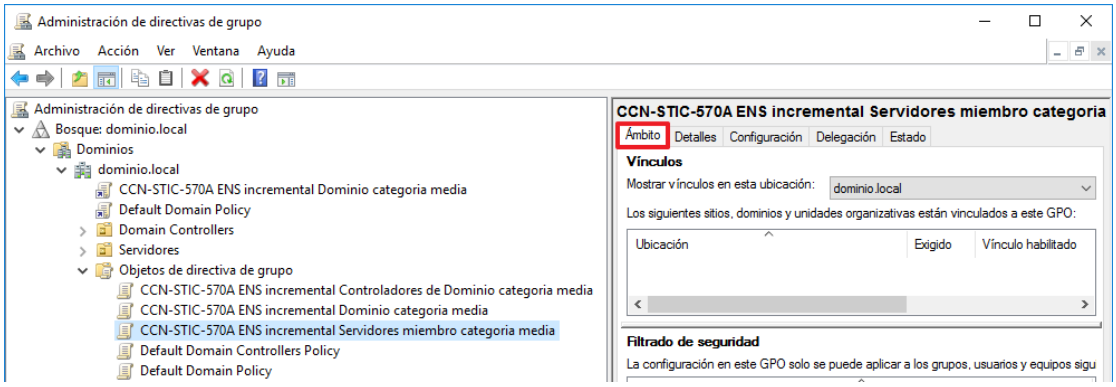
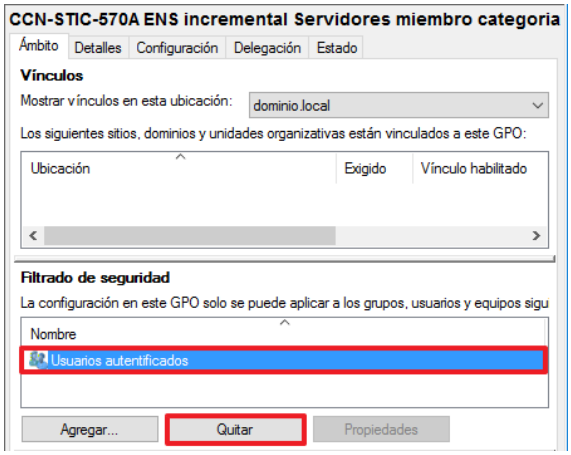
Paso	Descripción
15.	Introduzca el nombre de los servidores o utilice las opciones avanzadas para agregar todos aquellos servidores miembro que se encuentren afectados por el cumplimiento del ENS en su categoría de seguridad media y pulse el botón “Aceptar”.  **Nota:** No agregue controladores de dominio a este grupo.
16.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo.
17.	Cierre la herramienta de “Usuarios y equipos de Directorio Activo”.
18.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”** 
19.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”.

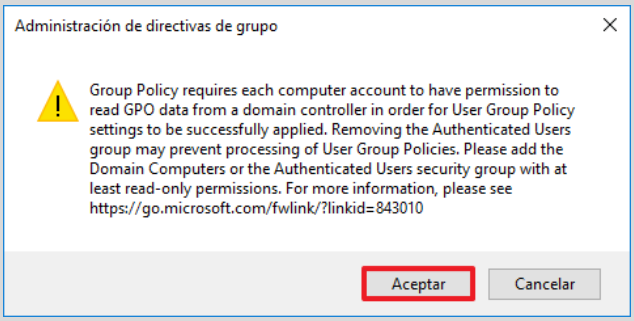
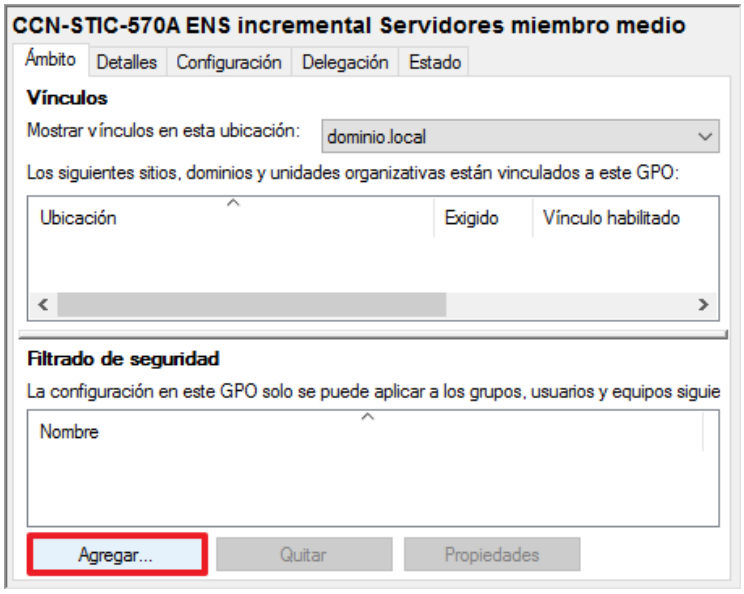
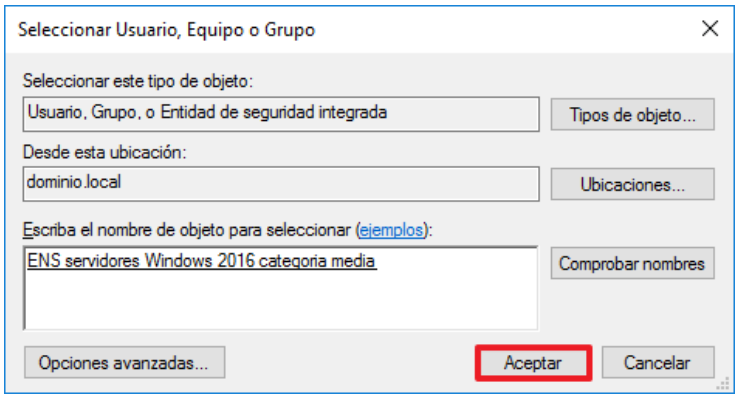
Paso	Descripción
20.	Pulse con el botón derecho, sobre dicha y carpeta y seleccione la opción “Nuevo”. 
21.	Introduzca como nombre “CCN-STIC-570A ENS incremental Servidores miembro categoria media” y pulse el botón “Aceptar”. 
22.	La nueva política requiere una configuración de plantillas administrativas. Para ello y seleccionando la política, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración…”. 
23.	En el asistente de importación de configuración, pulse el botón “Siguiente >”.
24.	En la selección de copia de seguridad, pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.
25.	En la “Carpeta de copia de seguridad”, pulse el botón “Examinar...”.

Paso	Descripción
26.	Seleccione la carpeta “CCN-STIC-570A ENS incremental Servidores categoria media” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 
27.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada.

Paso	Descripción
28.	En la pantalla siguiente compruebe que aparece la política de seguridad de servidores de categoría media y pulse el botón “Siguiente >”.  **Nota:** Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero “manifest.xml”. Este es un fichero oculto y, por lo tanto, debe mostrar en “opciones de carpeta”, la opción “Mostrar archivos, carpetas y unidades ocultos”. 
29.	En la pantalla de examen, pulse el botón “Siguiente >”.
30.	Si apareciera la ventana “Migrar referencias”, mantenga las opciones y pulse el botón “Siguiente >”.

Paso	Descripción
31.	Para completar el asistente pulse el botón “Finalizar”. 
32.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración.
33.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
34.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**
35.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva…”.

Paso	Descripción
36.	Seleccione de la ruta “C:\Windows\Security\Templates” el fichero “CCN-STIC-570A ENS incremental servidores categoria media” y pulse el botón “Abrir”. 
37.	Cierre la política de grupo.
38.	Seleccione la nueva política de grupo configurada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 
39.	De la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 

Paso	Descripción
40.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. **Nota:** En caso de que aparezca la siguiente advertencia ignórela y pulse “Aceptar”. 
41.	Una vez quitado, pulse el botón “Agregar…”. 
42.	Introduzca como nombre “ENS servidores Windows 2016 categoría media”. Este grupo corresponde con el generado en pasos previos. A continuación, pulse el botón “Aceptar”. 

Paso	Descripción
43.	Las políticas se encuentran ya creadas correctamente. No obstante, no se aplicarán hasta más adelante, una vez que haya tenido en cuenta y aplicado todas las consideraciones adicionales que se mostrarán en el siguiente punto del presente anexo. Cierre la herramienta "Administración de Directivas de Grupo".

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración. Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría media. No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

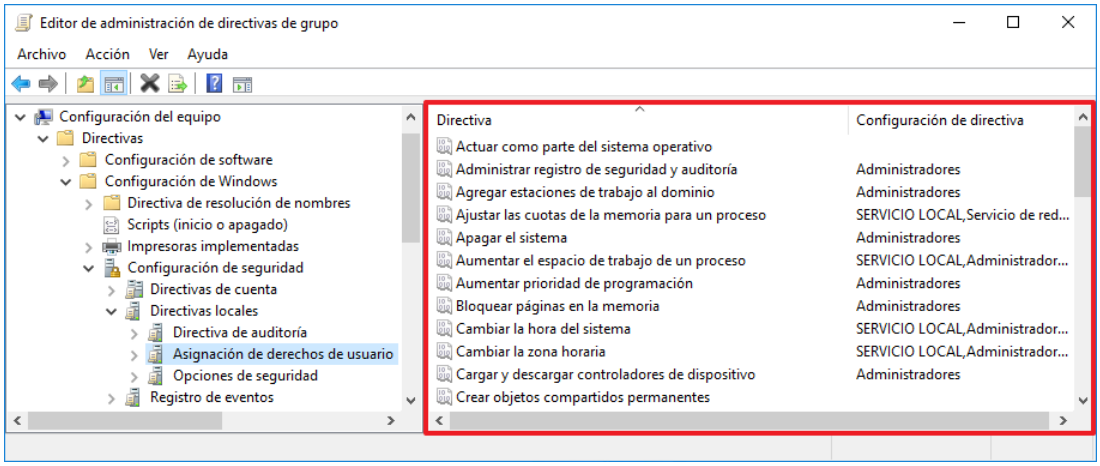
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

2.1. ASIGNACIÓN DE DERECHOS DE USUARIO

Los objetos de políticas de grupo para Controladores de Dominio y Servidores miembros especifican unos derechos de usuario siguiendo planteamientos de seguridad que aplican los principios de mínimo privilegio y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les hayan asignado derechos determinados para la administración o gestión de los sistemas.

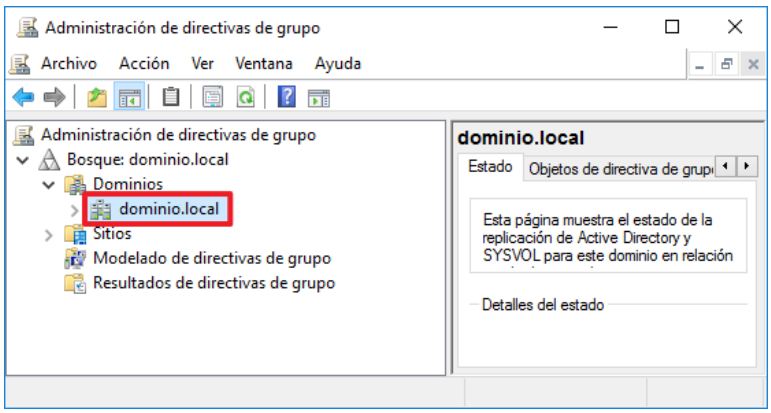
Si esto fuera así, deberá realizar las modificaciones pertinentes sobre el objeto de política de grupo "CCN-STIC-570A ENS incremental Servidores miembro categoria media".

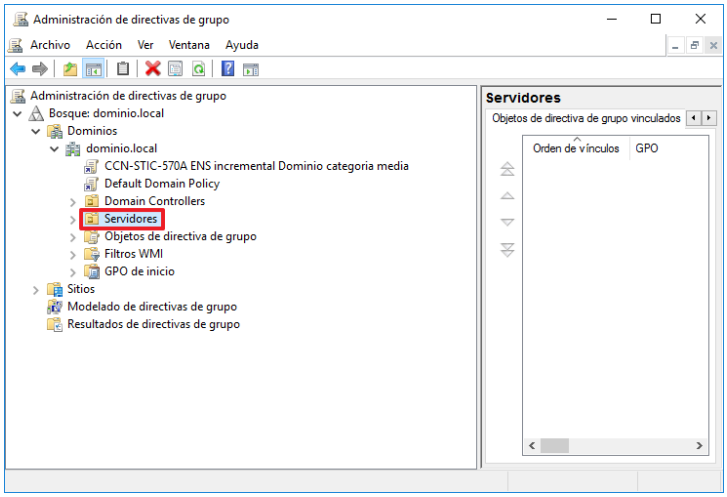
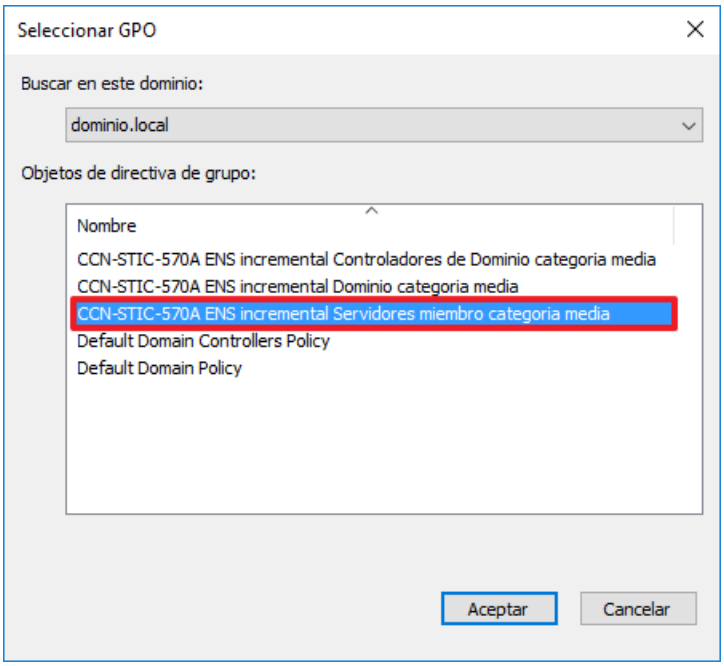
Paso	Descripción
44.	Edite la política de grupo correspondiente iniciando la herramienta "Administración de Directivas de Grupo" y seleccionando la política a modificar. Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"** Sobre el objeto de GPO que se quiere modificar, deberá pulsar clic derecho y seleccionar "Editar" en el menú desplegado.

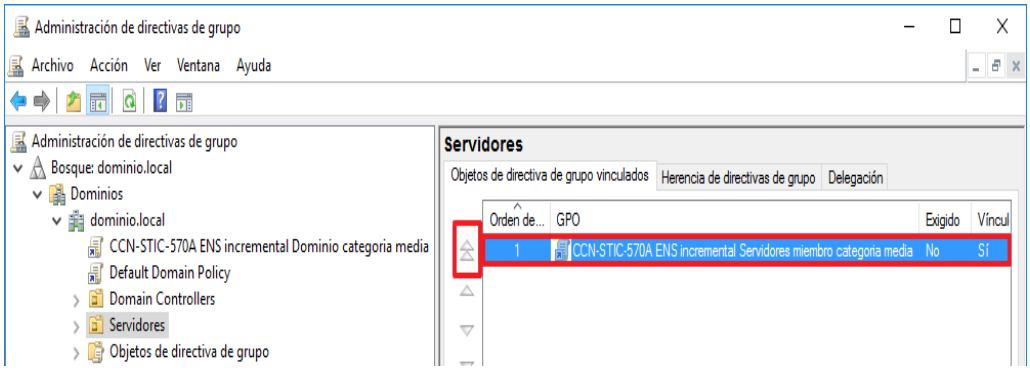
Paso	Descripción
45.	Una vez abierto el "Editor de administración de directivas de grupo", despliegue la política y sitúese en la siguiente ruta: **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"** 
46.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
47.	Guarde la configuración cerrando la ventana de editor de administración de directivas de grupo.

3. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

El presente punto establece la aplicación de las políticas de seguridad, toda vez que se han tenido en consideración las condiciones definidas en el punto previo.

Paso	Descripción
48.	Inicie la herramienta de administración de directivas de grupo.
49.	Despliegue el bloque y posiciónese sobre su dominio.  **Nota:** En el ejemplo el dominio utilizado se denomina "dominio.local".

Paso	Descripción
50.	Identifique las ubicaciones donde se encuentran los servidores Windows Server 2016 que les son de aplicación las condiciones de seguridad de categoría media, según estipula el ENS. Sobre cada una de esas ubicaciones, asigne el objeto de política de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria media”.  **Nota:** En el ejemplo se aplicará sobre la OU “Servidores”, que es donde se encuentran ubicados los servidores analizados en el escenario de test.
51.	Pulse con el botón derecho del ratón sobre la unidad organizativa correspondiente y selecciones la opción “Vincular un objeto GPO existente…”.
52.	Seleccione la política “CCN-STIC-570A ENS incremental Servidores miembro categoria media” y pulse el botón “Aceptar”. 

Paso	Descripción
53.	Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-570A ENS incremental Servidores miembro categoria media” y pulse el botón con la flecha que apunta hacia arriba hasta situarla en primer lugar dentro del orden de vínculo. 
54.	Repita los pasos 49 a 52 en cada una de las unidades organizativas donde se encuentren los servidores miembro Windows Server 2016 sujetos al cumplimiento del ENS en su categoría media.
55.	Cierre la herramienta de administración de directivas de grupo.
56.	Elimine la carpeta “C:\Scripts”.

4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD EN LOS EQUIPOS

Las configuraciones planteadas a través de la presente guía han sido ampliamente probadas en entornos de operativa Microsoft. No obstante, no se han podido probar todas las condiciones existentes, ni con las peculiaridades de cada organización. Bajo determinadas condiciones, pudieran suceder algunas incidencias que se describen a continuación, así como su resolución.

Debe tenerse en consideración que la resolución consiste en rebajar algunos de los mecanismos de seguridad descritos en la presente guía. Por lo tanto, deberá plantearse una solución que, de forma paulatina, permita alcanzar el estado de seguridad deseado y recomendado por la presente guía.

4.1. CONTROL DE CUENTAS DE USUARIO

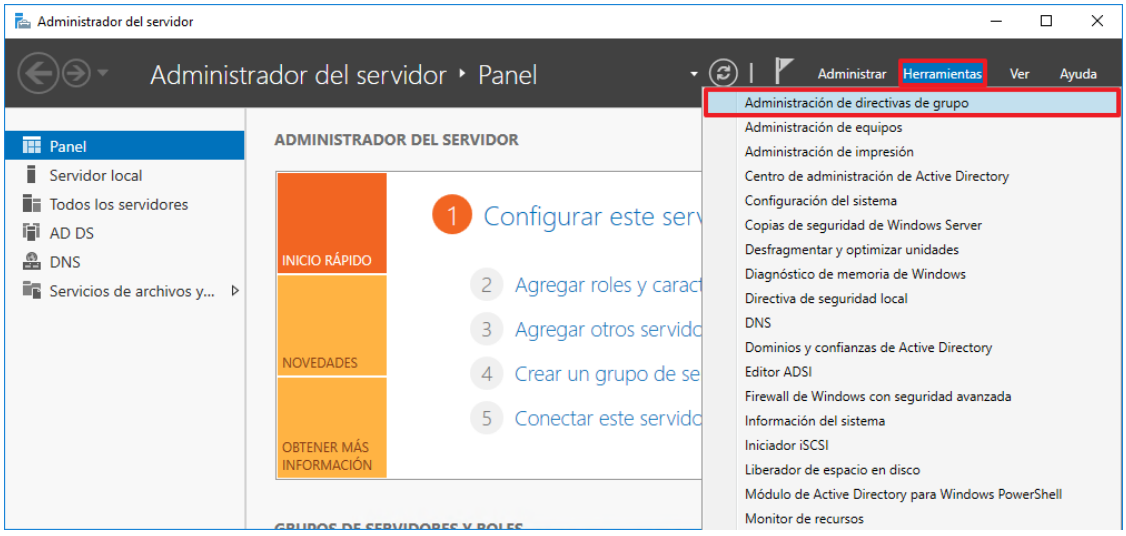
El control de cuentas de usuario surge en Windows Vista como respuesta para limitar las acciones de los administradores cuando actuaban con cuentas privilegiadas ante operativas que no requieren dicho privilegio. En sistemas previos a Windows Vista, un administrador que había iniciado una sesión actuaba siempre con los máximos privilegios, independientemente de que estuviera abriendo un fichero ofimático o estuviera navegando por internet. Puesto que el riesgo era bastante elevado, Microsoft propuso como solución UAC con objeto de advertir a los administradores cuando una acción requería privilegio para actuar.

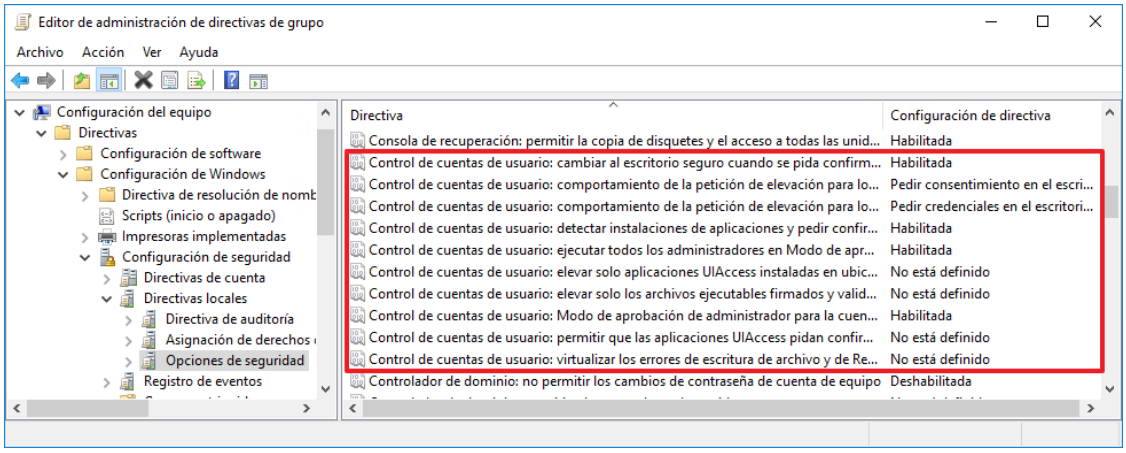
Siguiendo el principio de menor privilegio y menor exposición, la presente guía habilita las condiciones de funcionalidad de UAC para la categoría media, aunque con los criterios más laxos de los aplicables.

No obstante, ante aplicaciones o servicios antiguos pudieran darse fallos de funcionalidad en los mismos, requiriendo que se realicen análisis o la modificación en la configuración de UAC predeterminada para la categoría media por la presente guía.

Los siguientes pasos definen los procedimientos para la creación de una nueva política de seguridad de aplicación a los servidores que pudieran presentar incidencias con una nueva política de seguridad para el UAC.

Nota: La modificación deberá afectar exclusivamente a servidores miembro. Los controladores de dominio no deberían tener problemas en la ejecución de todos sus servicios en el modo de UAC habilitado.

Paso	Descripción
57.	Identifique los servidores que tienen problemas para la ejecución de aplicaciones y servicios y quítelos como miembros del grupo "ENS servidores Windows 2016 categoria media".
58.	Cree un nuevo grupo con nombre "ENS servidores miembro 2016 categoría media incidencias UAC", e incluya en dicho grupo los servidores miembro con una categoría media que presenten incidencias de funcionalidad del UAC. Realice estas tareas siguiendo los pasos 7 a 17 del presente anexo.
59.	Inicie la herramienta de "Administración de directivas de grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Inicio → Herramientas Administrativas → Administración de directivas de grupo"** 
60.	Cree una nueva política de grupo con el nombre "CCN-STIC-570A ENS incremental Servidores miembro categoria media incidencias UAC". Siga, para ello, los pasos 18 a 37 de este anexo. A continuación vincule el objeto de política de grupo a la unidad organizativa correspondiente siguiendo los pasos 48 a 55 de este anexo.
61.	Adicionalmente, asigne la nueva política de grupo al grupo de servidores recién creado "ENS servidores miembro 2016 categoria media incidencias UAC". Siga, para ello, los pasos 38 a 42 de este anexo.

Paso	Descripción
62.	Edite el nuevo objeto de GPO “CCN-STIC-570A ENS incremental Servidores miembro categoría media incidencias UAC”. Para ello seleccione dicha política y seleccione la opción “Editar…”
63.	Despliegue la política y sitúese en la siguiente ruta: **“Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**
64.	Identifique las directivas relativas a “Control de cuenta de usuario”. 
65.	Realice las modificaciones oportunas.
66.	Cierre la política.
67.	Para que la nueva política sea efectiva, necesita reiniciar el o los servidores. Esto es debido a que la aplicación se basa en la membresía a un grupo. La condición del miembro del grupo es adquirida por un equipo cuando inicia sesión en el dominio, cuestión que se produce cuando el equipo se reinicia. **Nota:** Debe tener en consideración que, si ha alterado la política de Control de cuentas de usuario y ésta es menos rigurosa que la propuesta en la configuración deseada por esta guía, se encuentra por debajo de los requerimientos de seguridad actuales. Debería evaluar los problemas ocasionados por las aplicaciones y servicios e intentar adaptarlos a configuraciones válidas. Es factible que si los servicios y/o aplicaciones no presentan funcionalidad con UAC presenten riesgos de seguridad notables y se esté exponiendo de forma significativa la infraestructura de la organización.

ANEXO A.3.4. LISTA DE COMPROBACIÓN DE WINDOWS SERVER 2016 COMO SERVIDOR MIEMBRO DE DOMINIO PARA LA CATEGORÍA MEDIA

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía "ANEXO A.3.3 GUÍA PASO A PASO SERVIDOR MIEMBRO QUE LE SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS".

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los dominios y servidores Windows Server 2016 con implementación de seguridad de categoría media del ENS.

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

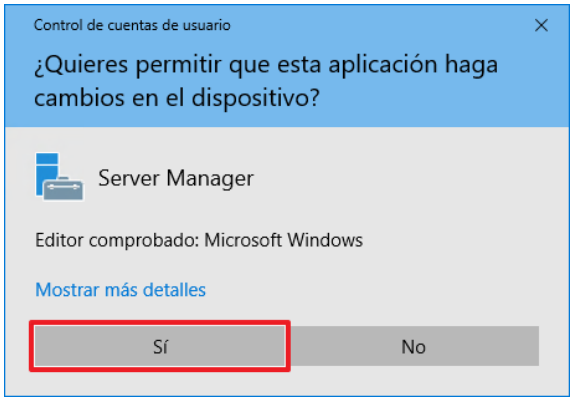
a) Administrador del Servidor

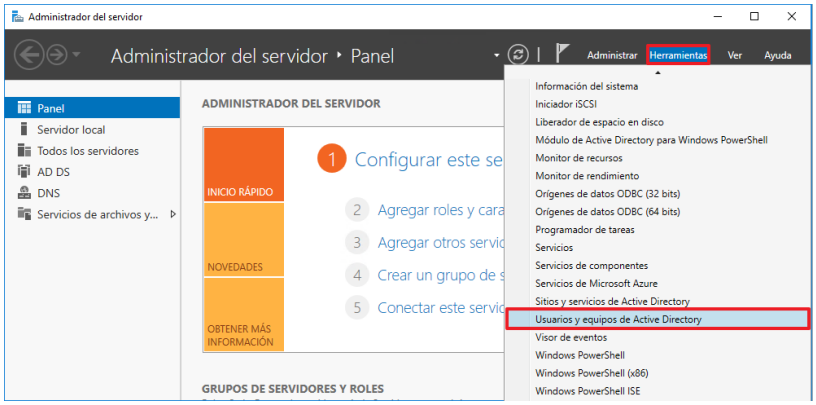
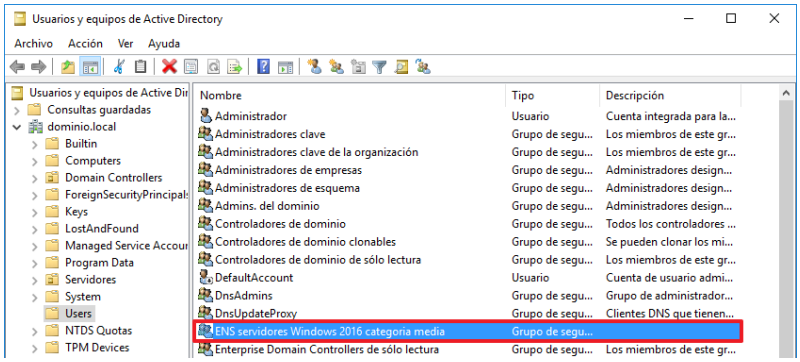
b) Conjunto resultante de directivas (rsop.msc)

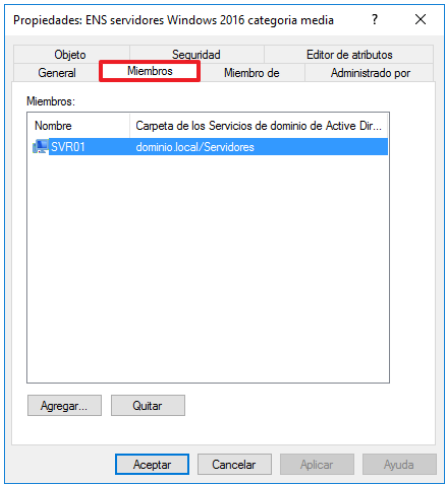
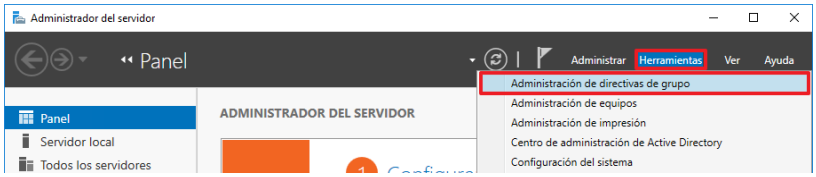
c) Consola de servicios (services.msc)

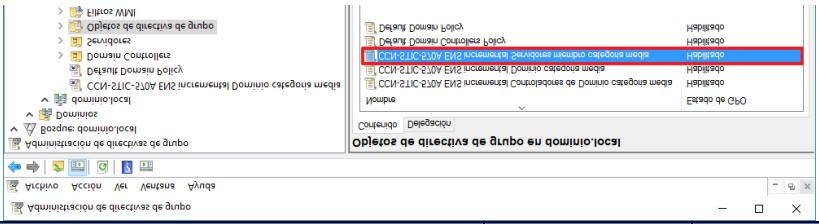
d) Editor de registro (regedit.exe)

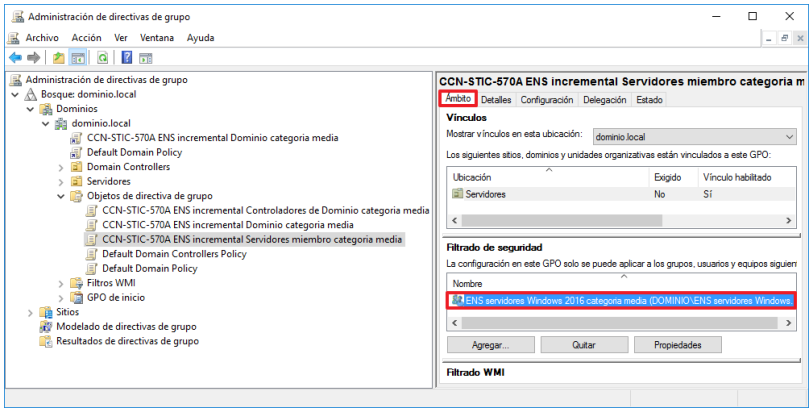
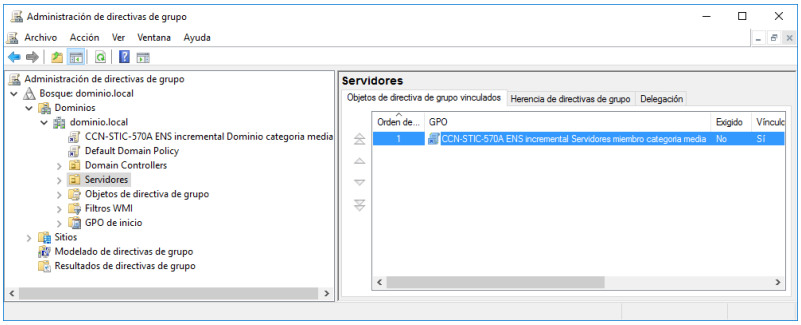
e) Explorador de Archivos (explorer.exe)

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

Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que está creado el grupo “ENS servidores Windows 2016 categoria media” dentro del contenedor “Users”.		Ejecute la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  Seleccione el contenedor “Users”, situado en la siguiente ruta: “**Usuarios y equipos de Active Directory → [Su dominio] → Users**” A continuación, en el panel de la derecha, verifique que está creado el objeto denominado “ENS servidores Windows 2016 categoria media”. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>3. Verifique que los servidores que han sido catalogados como de categoría de seguridad media y siguiendo los criterios definidos en el ENS, son miembros del grupo “ENS servidores Windows 2016 categoria media”.</td><td></td><td>Pulse doble clic sobre el grupo “ENS servidores Windows 2016 categoria media” situado en el panel de la derecha y seleccione la pestaña “Miembros” para verificar que los servidores que corresponden a esta categoría de seguridad aparecen en el listado.
 
</td></tr>
<tr><td>4. Verifique que los objetos de directivas de grupo han sido creados y están habilitados.</td><td></td><td>Ejecute la herramienta “Administrador de directivas de grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione:
“Herramientas → Administración de directivas de grupo”
 

Dentro de la consola diríjase a los “Objetos de directiva de grupo”:
“Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo”
Verifique que está creado el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria media” y que en la columna “Estado de GPO” figuran como habilitada.
 
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-570A ENS incremental Servidores miembro categoria media</td><td>Habilitado</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
5. Verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria media” tiene definido el Ámbito al grupo “ENS servidores Windows 2016 categoria media”		En el árbol de la izquierda, pulse doble clic sobre el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria media” desde: **“Bosques [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo”** Verifique en la pestaña “Ámbito” que dentro del campo “Filtrado de seguridad” figura el grupo “ENS servidores Windows 2016 categoria media”. 
6. Verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoría media” aplica a todos los objetos de las OU con servidores correspondientes a la categoría media según los criterios del ENS y ocupa el primer lugar en el orden de vinculación.		En el árbol de la izquierda sitúese sobre las unidades organizativas con servidores correspondientes a la categoría media según los criterios del ENS, en el ejemplo, “Servidores” desde: **“Bosque: [Su bosque] → Dominios → [Su Dominio] → Servidores”** En la pestaña “Objetos de Directiva de grupo vinculados” verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria media” figura en el panel de la derecha y ocupa el primer lugar en la columna “Orden de Vínculos”. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>7. Verifique los valores de auditoría de la directiva de grupo “CCN-STIC-570A ENS incremental servidores miembro categoria media”.</td><td></td><td>En el “Administrador de Directivas de Grupo” de uno de los controladores del dominio, pulse el botón derecho del ratón sobre la directiva desde:
“Bosque: [Su Bosque] → Dominios → [Su Dominio] → [OU de servidores] → CCN-STIC-570A ENS incremental servidores miembro categoria media”
Seleccione la opción “Editar…”. Cuando se abra el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Auditar el acceso a objetos</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar el acceso del servicio de directorio</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar el cambio de directivas</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar el seguimiento de procesos</td><td>Sin auditoría</td><td></td></tr>
<tr><td>Auditar el uso de privilegios</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar eventos de inicio de sesión</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar eventos de inicio de sesión de cuenta</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar eventos del sistema</td><td>Correcto</td><td></td></tr>
<tr><td>Auditar la administración de cuentas</td><td>Correcto, Erróneo</td><td></td></tr>
</table></td></tr>
<tr><td>8. Verifique los valores de asignación de derechos de usuario en la directiva de grupo “CCN-STIC-570A ENS incremental servidores miembro categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Administrar registro de seguridad y auditoría	Administradores	
		Agregar estaciones de trabajo al dominio	Administradores	
		Ajustar las cuotas de la memoria para un proceso	Administradores, SERVICIO LOCAL, Servicio de red	
		Apagar el sistema	Administradores	
		Aumentar el espacio de trabajo de un proceso	Administradores, SERVICIO LOCAL	
		Aumentar prioridad de programación	Administradores	
		Bloquear páginas en la memoria	Administradores	
		Cambiar la hora del sistema	SERVICIO LOCAL, Administradores	
		Cambiar la zona horaria	SERVICIO LOCAL, Administradores	
		Cargar y descargar controladores de dispositivo	Administradores	
		Crear Objetos globales	Administradores, SERVICIO, SERVICIO LOCAL, Servicio de red	
		Crear un archivo de paginación	Administradores	
		Crear vínculos simbólicos	Administradores	
		Denegar el acceso desde la red a este equipo	ANONYMOUS LOGON, Invitados	
		Denegar el inicio de sesión como servicio	Invitados	
		Denegar el inicio de sesión como trabajo por lotes	Invitados	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Denegar el inicio de sesión local	Invitados	
		Denegar el inicio de sesión a través de Servicios de Escritorio Remoto	Invitados	
		Forzar cierre desde un sistema remoto	Administradores	
		Generar auditorías de seguridad	SERVICIO LOCAL, Servicio de red	
		Generar perfiles de un solo proceso	Administradores	
		Generar perfiles de rendimiento del sistema	Administradores	
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	Administradores	
		Hacer copias de seguridad de archivos y directorios	Administradores, Operadores de copia de seguridad	
		Modificar la etiqueta de un objeto	Administradores	
		Modificar valores de entorno firmware	Administradores	
		Permitir el inicio de sesión local	Administradores	
		Quitar equipo de la estación de acoplamiento	Administradores	
		Realizar tareas de mantenimiento de volumen	Administradores	
		Reemplazar un símbolo (token) de nivel de proceso	SERVICIO LOCAL, Servicio de red	
		Restaurar archivos y directorios	Administradores	
		Suplantar a un cliente tras la autenticación	Administradores, SERVICIO, SERVICIO LOCAL, Servicio de red	
		Tener acceso a este equipo desde la red	Administradores, Usuarios autentificados, ENTERPRISE DOMAIN CONTROLLERS	
		Tomar posesión de archivos y otros objetos	Administradores	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>9. Verifique los valores de las opciones de seguridad de la directiva de grupo “CCN-STIC-570A ENS incremental servidores miembro categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de Seguridad”</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Acceso a redes: modelo de seguridad y uso compartido para cuentas locales</td><td>Clásico: usuarios locales se autentican con credenciales propias</td><td></td></tr>
<tr><td>Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos</td><td>Deshabilitada</td><td></td></tr>
<tr><td>Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: rutas del Registro accesibles remotamente</td><td>System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, Software\Microsoft\Windows NT\CurrentVersion</td><td></td></tr>
</table>
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Acceso a redes: rutas y subrutas del Registro accesibles remotamente	Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib, System\CurrentControlSet\Services\SysmonLog	
		Acceso de red: permitir traducción SID/nombre anónima	Deshabilitada	
		Apagado: borrar el archivo de paginación de la memoria virtual	Habilitada	
		Apagado: permitir apagar el sistema sin tener que iniciar sesión	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad	Habilitada	
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitada	
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitada	
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada	
		Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitada	
		Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitada	
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitada	
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitada	
		Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador	Pedir consentimiento	
		Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar	Pedir credenciales en el escritorio seguro	
		Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitada	
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitada	
		Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitada	
		Control de cuentas de usuario: Virtualizar los errores de escritura de archivo y de Registro en diferentes ubicaciones por usuario	Habilitada	
		Controlador de dominio: no permitir los cambios de contraseña de cuenta de equipo	Deshabilitada	
		Criptografía de sistema: forzar la protección con claves seguras para las claves de usuario almacenadas en el equipo	El usuario debe escribir una contraseña cada vez que use una clave	
		Cuentas: estado de la cuenta de invitado	Deshabilitada	
		Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitada	
		DCOM: restricciones de acceso al equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)	O:BAG:BAD: (A;;CCDCLC;;;AU)(A;;CCDCLC;;;S-1-5-32-562)	
		DCOM: restricciones de inicio al equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)	O:BAG:BAD: (A;;CCDCLCSWRP;;;BA)(A;;CCDCSW;;;AU)(A;;CCDCLCSWRP;;;S-1-5-32-562)	
		Dispositivos: impedir que los usuarios instalen controladores de impresora	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Dispositivos: impedir que los usuarios instalen controladores de impresora	Habilitada	
		Dispositivos: Permitir desacoplamiento sin tener que iniciar sesión	Deshabilitada	
		Dispositivos: permitir formatear y expulsar medios extraíbles	Administradores	
		Dispositivos: restringir el acceso a disquetes sólo al usuario con sesión iniciada localmente	Habilitada	
		Dispositivos: restringir el acceso al CD-ROM sólo al usuario con sesión iniciada localmente	Habilitada	
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo	
		Inicio de sesión interactivo: mostrar información de usuario cuando se bloquee la sesión	No mostrar la información del usuario	
		Inicio de sesión interactivo: no mostrar el último nombre de usuario	Habilitada	
		Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr	Deshabilitada	
		Inicio de sesión interactivo: número de inicios de sesión anteriores que se almacenarán en caché (si el controlador de dominio no está disponible	0 inicios de sesión	
		Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire	14 días	
		Inicio de sesión interactivo: requerir la autenticación del Controlador de Dominio para desbloquear la estación de trabajo	Habilitada	
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitada	
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitada	
		Miembro de dominio: duración máxima de contraseña de cuenta de equipo	30 días	
		Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	
		Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitada	
		Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitada	
		Seguridad de red: nivel de autenticación de LAN Manager	Enviar sólo respuesta NTLMv2 y rechazar LM	
		Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada	
		Seguridad de red: permitir que LocalSystem use la identidad del equipo para NTLM	Habilitada	
		Seguridad de red: permitir retroceso a sesión NULL de LocalSystem	Deshabilitada	
		Seguridad de red: permitir solicitudes de autenticación PKU2U a este equipo para usar identidades en Internet	Deshabilitada	
		Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma	
		Seguridad de red: restringir NTLM: auditar el tráfico NTLM entrante	Habilitar la auditoría para todas las cuentas	
		Seguridad de red: restringir NTLM: auditar la autenticación NTLM en este dominio	Habilitar todo	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td></td><td></td><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)</td><td>Habilitada</td><td></td></tr>
<tr><td>Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)</td><td>Habilitada</td><td></td></tr>
<tr><td>Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor</td><td>Requerido del cliente</td><td></td></tr>
<tr><td>Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión</td><td>15 minutos</td><td></td></tr>
</table></td></tr>
<tr><td rowspan="2">10. Verifique el registro de eventos de la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria media”.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro de eventos”</td></tr>
<tr><td></td><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Evitar que el grupo de invitados locales tenga acceso al registro de aplicaciones</td><td>Habilitada</td><td></td></tr>
<tr><td>Evitar que el grupo de invitados locales tenga acceso al registro de seguridad</td><td>Habilitada</td><td></td></tr>
<tr><td>Evitar que el grupo de invitados locales tenga acceso al registro del sistema</td><td>Habilitada</td><td></td></tr>
<tr><td>Método de retención del registro de la aplicación</td><td>Según se necesite</td><td></td></tr>
<tr><td>Método de retención del registro de seguridad</td><td>Según se necesite</td><td></td></tr>
<tr><td>Método de retención del registro del sistema</td><td>Según se necesite</td><td></td></tr>
<tr><td>Tamaño máximo del registro de la aplicación</td><td>32768 kilobytes</td><td></td></tr>
<tr><td>Tamaño máximo del registro de seguridad</td><td>163840 kilobytes</td><td></td></tr>
<tr><td>Tamaño máximo del registro del sistema</td><td>32768 kilobytes</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
11. Verifique los servicios de sistema en la directiva de grupo "CCN-STIC-570A ENS incremental Servidores miembro categoria media".		Seleccione el siguiente nodo. **"Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"** **Nota:** Dependiendo de los servicios que estén instalados en el equipo, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales (antivirus, etc.). En la siguiente tabla se muestran el nombre largo y el nombre corto para cada servicio. En la ventana del editor de administración de directivas de grupo sólo aparecerá uno de los dos: el nombre largo si el servicio está instalado en el sistema o el nombre corto si no lo está. Además, deberá tener en cuenta que los números existentes en algunos servicios son aleatorios y cambian en cada equipo.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado	
Administración de aplicaciones	AppMgmt	Manual	Configurado	
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado	
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado	
Administración remota de Windows (WS-Management)	WinRM	Automático	Configurado	
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado	
Administrador de conexiones de acceso remoto	RasMan	Manual	Configurado	
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado	

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK

Comprobación	OK/NOK	Cómo hacerlo		
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado	
Administrador de credenciales	VaultSvc	Manual	Configurado	
Administrador de cuentas de seguridad	SamSs	Automático	Configurado	
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado	
Administrador de sesión local	LSM	Automático	Configurado	
Administrador de usuarios	UserManager	Automático	Configurado	
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado	
Agente de conexión de red	NcbService	Manual	Configurado	
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado	
Agente de directiva IPsec	PolicyAgent	Manual	Configurado	
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado	
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado	
Aislamiento de claves CNG	KeyIso	Manual	Configurado	
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado	
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado	
Aplicación auxiliar IP	iphlpsvc	Automático	Configurado	
Aplicación del sistema COM+	COMSysApp	Manual	Configurado	
Archivos sin conexión	CscService	Deshabilitado	Configurado	
Asignador de detección de topologías de nivel de vínculo	lltdsvc	Manual	Configurado	
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Asistente para la conectividad de red	NcaSvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Audio de Windows	Audiosrv	Manual	Configurado	
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Deshabilitado	Configurado	
Ayudante especial de la consola de administración	sacsvr	Manual	Configurado	
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado	
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado	
CDPUserSvc	CDPUserSvc	Automático	Configurado	
Cliente de directiva de grupo	gpsvc	Automático	Configurado	
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático	Configurado	
Cliente DHCP	Dhcp	Automático	Configurado	
Cliente DNS	Dnscache	Automático	Configurado	
Cola de impresión	Spooler	Automático	Configurado	
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Manual	Configurado	
Comprobador puntual	svsvc	Manual	Configurado	
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado	
Conexiones de red	Netman	Manual	Configurado	
Configuración automática de redes cableadas	dot3svc	Manual	Configurado	
Configuración de Escritorio remoto	SessionEnv	Manual	Configurado	
Conjunto resultante de proveedor de directivas	RSoPProv	Manual	Configurado	
Contenedor de Microsoft Passport	NgcCtnrSvc	Manual	Configurado	
Coordinador de transacciones distribuidas	MSDTC	Automático	Configurado	
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
DataCollectionPublishingService	DcpSvc	Manual	Configurado	
Datos de contactos	PimIndexMaintenanceS	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
	vc			
Detección de hardware shell	ShellHWDetection	Deshabilitado	Configurado	
Detección de servicios interactivos	UI0Detect	Manual	Configurado	
Detección SSDP	SSDPSRV	Deshabilitado	Configurado	
Directiva de extracción de tarjetas inteligentes	SCPolicySvc	Manual	Configurado	
Disco virtual	vds	Manual	Configurado	
Dispositivo host de UPnP	upnphost	Manual	Configurado	
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado	
dmwappushsvc	dmwappushservice	Deshabilitado	Configurado	
Energía	Power	Automático	Configurado	
Enrutamiento y acceso remoto	RemoteAccess	Deshabilitado	Configurado	
Estación de trabajo	LanmanWorkstation	Automático	Configurado	
Eventos de adquisición de imágenes estáticas	WiaRpc	Manual	Configurado	
Examinador de equipos	Browser	Deshabilitado	Configurado	
Experiencia de calidad de audio y vídeo de Windows (qWave)	QWAVE	Deshabilitado	Configurado	
Extensiones y notificaciones de impresora	PrintNotify	Manual	Configurado	
Firewall de Windows	MpsSvc	Automático	Configurado	
Hora de Windows	W32Time	Automático	Configurado	
Host de proveedor de detección de función	fdPHost	Deshabilitado	Configurado	
Host de sistema de diagnóstico	WdiSystemHost	Deshabilitado	Configurado	
Host del servicio de diagnóstico	WdiServiceHost	Deshabilitado	Configurado	
Identidad de aplicación	AppIDSvc	Manual	Configurado	
Información de la aplicación	Appinfo	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Iniciador de procesos de servidor DCOM	DcomLaunch	Automático	Configurado	
Inicio de sesión secundario	seclogon	Deshabilitado	Configurado	
Instalador de ActiveX	AxInstSV	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
(AxInstSV)					
Instalador de módulos de Windows	TrustedInstaller	Manual	Configurado		
Instantáneas de volumen	VSS	Manual	Configurado		
Instrumental de administración de Windows	Winmgmt	Automático	Configurado		
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado		
KTMRM para DTC (Coordinador de transacciones distribuidas)	KtmRm	Manual	Configurado		
Llamada a procedimiento remoto (RPC)	RpcSs	Automático	Configurado		
Microsoft App-V Client	AppVClient	Deshabilitado	Configurado		
Microsoft Passport	NgcSvc	Manual	Configurado		
Modo incrustado	embeddedmode	Manual	Configurado		
Módulos de creación de claves de IPsec para IKE y AuthIP	IKEEXT	Manual	Configurado		
Motor de filtrado de base	BFE	Automático	Configurado		
Net Logon	Netlogon	Automático	Configurado		
Optimizar unidades	defragsvc	Manual	Configurado		
Partida guardada en Xbox Live	XblGameSave	Deshabilitado	Configurado		
Plug and Play	PlugPlay	Manual	Configurado		
Preparación de aplicaciones	AppReadiness	Manual	Configurado		
Programador de tareas	Schedule	Automático	Configurado		
Propagación de certificados	CertPropSvc	Manual	Configurado		
Protección de software	sppsvc	Automático	Configurado		

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Protocolo de autenticación extensible	Eaphost	Manual	Configurado	
Proveedor de instantáneas de software de Microsoft	swprv	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Publicación de recurso de detección de función	FDResPub	Deshabilitado	Configurado	
Reconoc. ubicación de red	NlaSvc	Automático	Configurado	
Recopilador de eventos de Windows	Wecsvc	Manual	Configurado	
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService	Manual	Configurado	
Registro de eventos de Windows	EventLog	Automático	Configurado	
Registro remoto	RemoteRegistry	Deshabilitado	Configurado	
Registros y alertas de rendimiento	pla	Manual	Configurado	
Servicio Asistente para la compatibilidad de programas	PcaSvc	Automático	Configurado	
Servicio biométrico de Windows	WbioSrvc	Manual	Configurado	
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc	Manual	Configurado	
Servicio de administración de aplicaciones de empresa	EntAppSvc	Manual	Configurado	
Servicio de administración de radio	RmSvc	Manual	Configurado	
Servicio de administrador de licencias de Windows	LicenseManager	Manual	Configurado	
Servicio de almacenamiento	StorSvc	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de asociación de dispositivos	DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows	FontCache	Deshabilitado	Configurado	
Servicio de cierre de invitado de Hyper-V	vmicshutdown	Manual	Configurado	
Servicio de	bthserv	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
compatibilidad con Bluetooth				
Servicio de configuración de red	NetSetupSvc	Manual	Configurado	
Servicio de datos del sensor	SensorDataService	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP	WinHttpAutoProxySvc	Manual	Configurado	
Servicio de directivas de diagnóstico	DPS	Deshabilitado	Configurado	
Servicio de dispositivo de interfaz humana	hidserv	Manual	Configurado	
Servicio de enrutador de AllJoyn	AJRouter	Deshabilitado	Configurado	
Servicio de enumeración de dispositivos de tarjeta inteligente	ScDeviceEnum	Manual	Configurado	
Servicio de geolocalización	lfsvc	Manual	Configurado	
Servicio de host HV	HvHost	Manual	Configurado	
Servicio de implementación de AppX (AppXSVC)	AppXSvc	Manual	Configurado	
Servicio de infraestructura de tareas en segundo plano	BrokerInfrastructure	Automático	Configurado	
Servicio de inscripción de administración de dispositivos	DmEnrollmentSvc	Manual	Configurado	
Servicio de inspección de red de Windows Defender	WdNisSvc	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de instalación de dispositivos	DeviceInstall	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado	
Servicio de licencia de cliente (ClipSVC)	ClipSVC	Manual	Configurado	
Servicio de lista de	netprofm	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
redes					
Servicio de notificación de eventos de sistema	SENS		Automático	Configurado	
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService		Deshabilitado	Configurado	
Servicio de perfil de usuario	ProfSvc		Automático	Configurado	
Servicio de plataforma de dispositivos conectados	CDPSvc		Automático	Configurado	
Servicio de protocolo de túnel de sockets seguros	SstpSvc		Manual	Configurado	
Servicio de puerta de enlace de nivel de aplicación	ALG		Manual	Configurado	
Servicio de registro de acceso de usuarios	UALSVC		Automático	Configurado	
Servicio de repositorio de estado	StateRepository		Manual	Configurado	
Servicio de sensores	SensorService		Manual	Configurado	
Servicio de servidor proxy KDC (KPS)	KPSSVC		Manual	Configurado	
Servicio de sincronización de hora de Hyper-V	vmictimesync		Manual	Configurado	
Servicio de supervisión de licencias de Windows	WLMS		Automático	Configurado	
Servicio de supervisión de sensores	SensrSvc		Manual	Configurado	

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Manual	Configurado	
Servicio de uso compartido de datos	DsSvc	Manual	Configurado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Deshabilitado	Configurado	
Servicio de usuario de	WpnUserService	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
notificaciones de inserción de Windows					
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual	Configurado		
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado		
Servicio de Windows Defender	WinDefend	Automático	Configurado		
Servicio de Windows Insider	wisvc	Manual	Configurado		
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado		
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Manual	Configurado		
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado		
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Manual	Configurado		
Servicio FrameServer de la Cámara de Windows	FrameServer	Manual	Configurado		
Servicio host de proveedor de cifrado de Windows	WEPHOSTSVC	Manual	Configurado		
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**	
Servicio Interfaz de almacenamiento en red	nsi	Automático	Configurado		
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado		
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standardcollector.service	Manual	Configurado		
Servicio telefónico	PhoneSvc	Manual	Configurado		
Servicios de cifrado	CryptSvc	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicios de Escritorio remoto	TermService		Manual	Configurado	
Servidor	LanmanServer		Automático	Configurado	
Servidor del modelo de datos del mosaico	tiledatamodelsvc		Automático	Configurado	
Sincronizar host	OneSyncSvc		Automático	Configurado	
Sistema de cifrado de archivos (EFS)	EFS		Manual	Configurado	
Sistema de eventos COM+	EventSystem		Automático	Configurado	
SMP de Espacios de almacenamiento de Microsoft	smphost		Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V	vmicvss		Manual	Configurado	
Superfetch	SysMain		Manual	Configurado	
Tarjeta inteligente	SCardSvr		Deshabilitado	Configurado	
Telefonía	TapiSrv		Deshabilitado	Configurado	
Telemetría y experiencias del usuario conectado	DiagTrack		Automático	Configurado	
Temas	Themes		Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)	RpcLocator		Manual	Configurado	
WalletService	WalletService		Manual	Configurado	
Windows Driver Foundation - User-mode Driver Framework	wudfsvc		Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**		**Inicio**	**Permiso**	**OK/NOK**
Windows Installer	msiserver		Manual	Configurado	
Windows Search	WSearch		Deshabilitado	Configurado	
Windows Update	wuauserv		Manual	Configurado	
SMP de Espacios de almacenamiento de Microsoft	smphost		Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V	vmicvss		Manual	Configurado	
Superfetch	SysMain		Manual	Configurado	
Tarjeta inteligente	SCardSvr		Deshabilitado	Configurado	
Telefonía	TapiSrv		Deshabilitado	Configurado	
Telemetría y	DiagTrack		Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
experiencias del usuario conectado					
Temas		Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)		RpcLocator	Manual	Configurado	
WalletService		WalletService	Manual	Configurado	
Windows Driver Foundation - User-mode Driver Framework		wudfsvc	Manual	Configurado	
Windows Installer		msiserver	Manual	Configurado	
12. Verifique los permisos de valores de registro de la directiva de grupo "CCN-STIC-570A ENS incremental Servidores miembro categoria media".		Seleccione el siguiente nodo. **"Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro"** **Nota**: Para verificar los permisos de la entrada de registro, deberá pulsar doble clic sobre la entrada **"MACHINES → SOFTWARE → Microsoft → Windows → CurrentVersion → Installer"** y pulsar sobre el botón "Modificar seguridad...". Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".			
		Directiva	**Valor**	**OK/NOK**	
		MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer	Administradores: Control Total SYSTEM: Control Total Usuarios: Leer		
13. Verifique los valores del sistema de archivos de la directiva de grupo "CCN-STIC-570A ENS incremental Servidores miembro categoria media".		Seleccione el siguiente nodo. **"Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de Archivos"** **Nota**: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción "Propiedades" del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...". Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".			

Comprobación	OK/NOK	Cómo hacerlo

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\Registration	Administrador	Control total	
	System	Control total	
	Usuario	Leer y ejecutar	
%SystemRoot%\repair	Administrador	Control total	
	System	Control total	
%SystemRoot%\security	Administrador	Control total	
	System	Control total	
SystemRoot%\system32\cacls	Administrador	Control total	
	System	Control total	
SystemRoot%\system32\clip.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\ras	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\rasadhlp.dll	Administrador	Control total	
%SystemRoot%\system32\rasauto.dll	Administrador	Control total	
%SystemRoot%\system32\rasautou.exe	Administrador	Control total	
%SystemRoot%\system32\raschap.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrnm.h	Administrador	Control total	
%SystemRoot%\system32\rasctrs.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrs.ini	Administrador	Control total	
%SystemRoot%\system32\rasdial	Administrador	Control total	
%SystemRoot%\system32\rasmans.dll	Administrador	Control total	
%SystemRoot%\system32\rasmontr.dll	Administrador	Control total	
%SystemRoot%\system32\rasphone.exe	Administrador	Control total	
%SystemRoot%\system32\rasppp.dll	Administrador	Control total	
%SystemRoot%\system32\rastapi.dll	Administrador	Control total	
%SystemRoot%\system32\rastls.dll	Administrador	Control total	

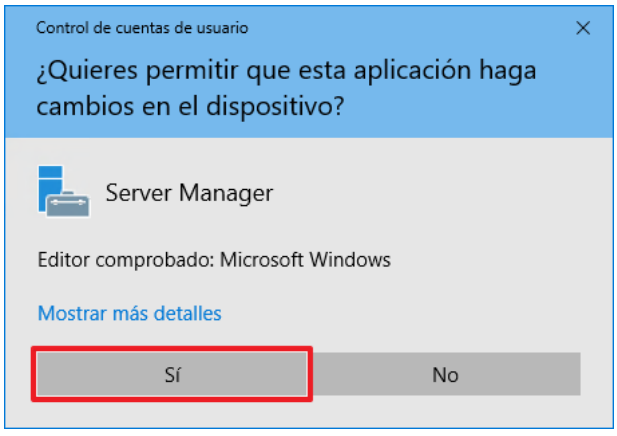
Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\system32\runonce.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\secedit.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\telnet.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tftp.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tracert.exe	Administrador	Control total	
	System	Control total	

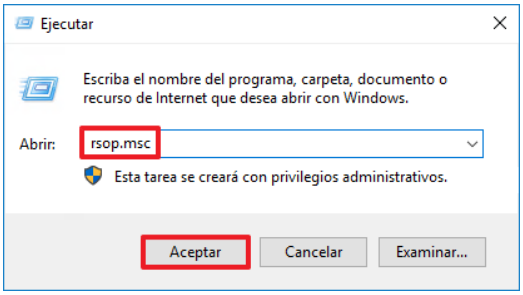
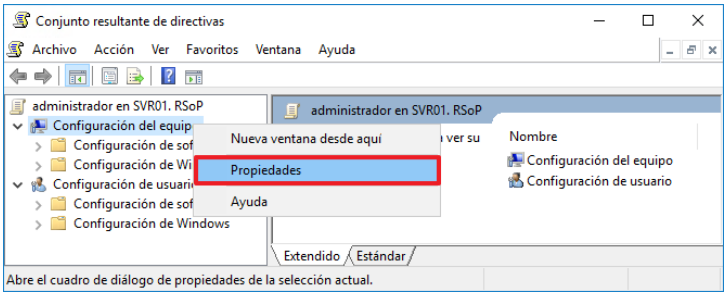
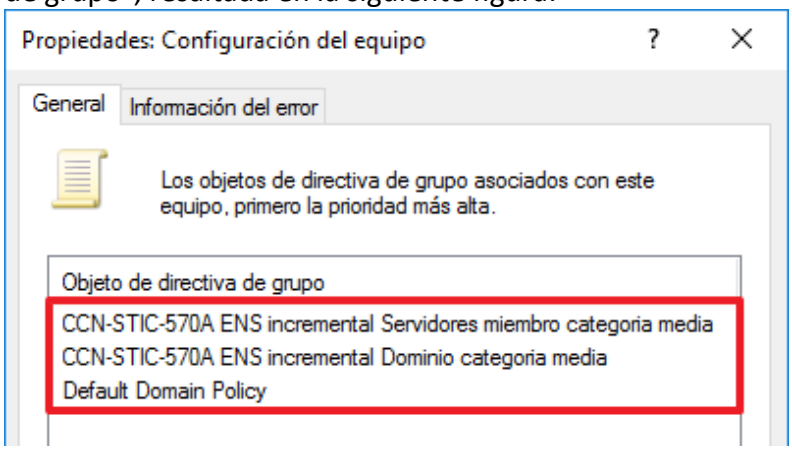
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td rowspan="3">14. Verifique que está bloqueada la ejecución del Almacén digital en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Administración de derechos digitales de Windows Media”</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Impedir el acceso a internet de Windows Media DRM</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td></td></tr>
<tr><td rowspan="3">15. Verifique que está bloqueada la ejecución del Almacén digital en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Almacén Digital”</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>No permitir que se ejecute el Almacén digital</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td></td></tr>
</table>

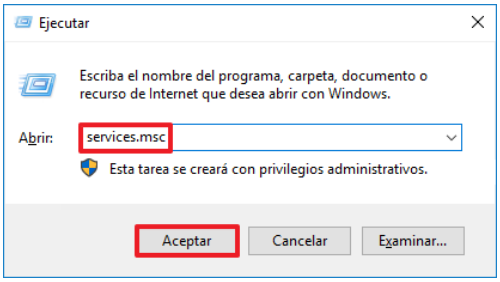
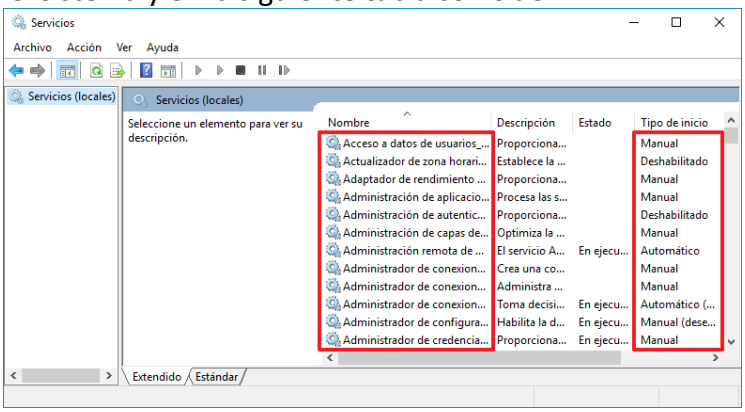
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>16. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Biometría”</td></tr>
<tr><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Permitir el uso de biometría</td><td>Habilitada</td><td></td></tr>
<tr><td>Permitir que los usuarios de dominio inicien sesión mediante biometría</td><td>Habilitada</td><td></td></tr>
<tr><td>Permitir que los usuarios inicien sesión mediante biometría</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td>17. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Directivas de reproducción automática”</td></tr>
<tr><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Desactivar reproducción automática</td><td>Habilitada</td><td></td></tr>
<tr><td>Comportamiento predeterminado para la ejecución automática</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>18. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Informe de errores de Windows”</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Deshabilitar el informe de errores de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td>No enviar datos adicionales</td><td>Habilitada</td><td></td></tr>
</table>
</td></tr>
<tr><td>19. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria media”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Opciones de inicio de sesión de Windows”</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario</td><td>Habilitada</td><td></td></tr>
<tr><td>Informar cuando el servidor de inicio de sesión no está disponible durante el inicio de sesión del usuario</td><td>Habilitada</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td rowspan="3">20. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria media”.</td><td></td><td colspan="2">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Shell remoto de Windows”</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Permitir acceso a Shell remoto</td><td>Deshabilitada</td><td></td></tr>
</table></td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="3">21. Verifique configuración de la comunicación de Internet en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria media”.</td><td></td><td colspan="2">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Desactivar informe de errores de reconocimiento de escritura a mano</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el Programa para la mejora de la experiencia del usuario de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar los vínculos “Events.asp” del Visor de eventos</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el contenido “¿Sabía que…?” del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la búsqueda en Microsoft Knowledge Base del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el informe de errores de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la actualización de archivos de contenido del Asistente para búsqueda</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td></td><td></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Desactivar el acceso a la Tienda</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la tarea de imágenes “Pedir copias fotográficas”</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td rowspan="2">22. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria media”.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Sistema → Net Logon”</td></tr>
<tr><td colspan="4"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Permitir algoritmos de criptografía compatibles con Windows NT 4.0</td><td>Deshabilitada</td><td></td></tr>
</table></td></tr>
<tr><td>23. Inicie sesión en el servidor a comprobar.</td><td></td><td colspan="3">Inicie sesión con una cuenta que tenga privilegios de administración del dominio en el servidor a comprobar.
El sistema solicitará elevación de privilegios para poder ejecutar el “Administrador del Servidor”. Pulse “Sí” en la ventana de “Control de cuentas de usuario”
 
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
24. Verifique que el equipo ha recibido la directiva de grupo CCN-STIC-570A ENS incremental Servidores miembro categoria media.		Ejecute la consola de administración "Conjunto resultante de directivas" (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → rsop.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" en la ventana que se muestra a continuación:  Seleccione en ella la rama "Configuración del equipo", márquela con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la figura:  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", resaltada en la siguiente figura:  Verifique que en dicha sección aparecen listados, y por ese orden, los objetos de directiva de grupo que se indican en la siguiente tabla:

Comprobación	OK/NOK	Cómo hacerlo
	Objeto de directiva de grupo	OK/NOK
	CCN-STIC-570A ENS incremental Servidores miembro categoria media	
	CCN-STIC-570A ENS incremental Dominio categoria media	
	Default Domain Policy	
25. Verifique que los servicios del sistema están correctamente configurados		Usando la consola de servicios (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → services.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" para continuar.  Verifique que el tipo de inicio de los servicios que aparecen en el sistema y en la siguiente tabla coinciden:  **Nota:** Dependiendo del equipo, es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales (antivirus, etc.).

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado	
Administración de aplicaciones	AppMgmt	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**

Comprobación	OK/NOK	Cómo hacerlo			
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado		
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado		
Administración remota de Windows (WS-Management)	WinRM	Automático	Configurado		
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado		
Administrador de conexiones de acceso remoto	RasMan	Manual	Configurado		
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado		
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado		
Administrador de credenciales	VaultSvc	Manual	Configurado		
Administrador de cuentas de seguridad	SamSs	Automático	Configurado		
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado		
Administrador de sesión local	LSM	Automático	Configurado		
Administrador de usuarios	UserManager	Automático	Configurado		
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado		
Agente de conexión de red	NcbService	Manual	Configurado		
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado		
Agente de directiva IPsec	PolicyAgent	Manual	Configurado		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**	
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado	
Aislamiento de claves CNG	KeyIso	Manual	Configurado	
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado	
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado	
Aplicación auxiliar IP	iphlpsvc	Automático	Configurado	
Aplicación del sistema COM+	COMSysApp	Manual	Configurado	
Archivos sin conexión	CscService	Deshabilitado	Configurado	
Asignador de detección de topologías de nivel de vínculo	lltdsvc	Manual	Configurado	
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado	
Asistente para la conectividad de red	NcaSvc	Manual	Configurado	
Audio de Windows	Audiosrv	Manual	Configurado	
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Deshabilitado	Configurado	
Ayudante especial de la consola de administración	sacsvr	Manual	Configurado	
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado	
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado	
CDPUserSvc	CDPUserSvc	Automático	Configurado	
Cliente de directiva de grupo	gpsvc	Automático	Configurado	
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático	Configurado	
Cliente DHCP	Dhcp	Automático	Configurado	
Cliente DNS	Dnscache	Automático	Configurado	
Cola de impresión	Spooler	Automático	Configurado	
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Comprobador puntual	svsvc	Manual	Configurado	
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Conexiones de red	Netman	Manual	Configurado	
Configuración automática de redes cableadas	dot3svc	Manual	Configurado	
Configuración de Escritorio remoto	SessionEnv	Manual	Configurado	
Conjunto resultante de proveedor de directivas	RSoPProv	Manual	Configurado	
Contenedor de Microsoft Passport	NgcCtnrSvc	Manual	Configurado	
Coordinador de transacciones distribuidas	MSDTC	Automático	Configurado	
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado	
DataCollectionPublishingService	DcpSvc	Manual	Configurado	
Datos de contactos	PimIndexMaintenanceSvc	Manual	Configurado	
Detección de hardware shell	ShellHWDetection	Deshabilitado	Configurado	
Detección de servicios interactivos	UI0Detect	Manual	Configurado	
Detección SSDP	SSDPSRV	Deshabilitado	Configurado	
Directiva de extracción de tarjetas inteligentes	SCPolicySvc	Manual	Configurado	
Disco virtual	vds	Manual	Configurado	
Dispositivo host de UPnP	upnphost	Manual	Configurado	
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado	
dmwappushsvc	dmwappushservice	Deshabilitado	Configurado	
Energía	Power	Automático	Configurado	
Enrutamiento y acceso remoto	RemoteAccess	Deshabilitado	Configurado	
Estación de trabajo	LanmanWorkstation	Automático	Configurado	
Eventos de adquisición de imágenes estáticas	WiaRpc	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Examinador de equipos	Browser	Deshabilitado	Configurado	
Experiencia de calidad de audio y vídeo de Windows (qWave)	QWAVE	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Extensiones y notificaciones de impresora	PrintNotify	Manual	Configurado		
Firewall de Windows	MpsSvc	Automático	Configurado		
Hora de Windows	W32Time	Automático	Configurado		
Host de proveedor de detección de función	fdPHost	Deshabilitado	Configurado		
Host de sistema de diagnóstico	WdiSystemHost	Deshabilitado	Configurado		
Host del servicio de diagnóstico	WdiServiceHost	Deshabilitado	Configurado		
Identidad de aplicación	AppIDSvc	Manual	Configurado		
Información de la aplicación	Appinfo	Manual	Configurado		
Iniciador de procesos de servidor DCOM	DcomLaunch	Automático	Configurado		
Inicio de sesión secundario	seclogon	Deshabilitado	Configurado		
Instalador de ActiveX (AxInstSV)	AxInstSV	Manual	Configurado		
Instalador de módulos de Windows	TrustedInstaller	Manual	Configurado		
Instantáneas de volumen	VSS	Manual	Configurado		
Instrumental de administración de Windows	Winmgmt	Automático	Configurado		
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado		
KTMRM para DTC (Coordinador de transacciones distribuidas)	KtmRm	Manual	Configurado		
Llamada a procedimiento remoto (RPC)	RpcSs	Automático	Configurado		
Microsoft App-V Client	AppVClient	Deshabilitado	Configurado		
Microsoft Passport	NgcSvc	Manual	Configurado		
Modo incrustado	embeddedmode	Manual	Configurado		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**	
Módulos de creación de claves de IPsec para IKE y AuthIP	IKEEXT	Manual	Configurado		
Motor de filtrado de base	BFE	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Net Logon		Netlogon	Automático	Configurado	
Optimizar unidades		defragsvc	Manual	Configurado	
Partida guardada en Xbox Live		XblGameSave	Deshabilitado	Configurado	
Plug and Play		PlugPlay	Manual	Configurado	
Preparación de aplicaciones		AppReadiness	Manual	Configurado	
Programador de tareas		Schedule	Automático	Configurado	
Propagación de certificados		CertPropSvc	Manual	Configurado	
Protección de software		sppsvc	Automático	Configurado	
Protocolo de autenticación extensible		Eaphost	Manual	Configurado	
Proveedor de instantáneas de software de Microsoft		swprv	Manual	Configurado	
Publicación de recurso de detección de función		FDResPub	Deshabilitado	Configurado	
Reconoc. ubicación de red		NlaSvc	Automático	Configurado	
Recopilador de eventos de Windows		Wecsvc	Manual	Configurado	
Redirector de puerto en modo usuario de Servicios de Escritorio remoto		UmRdpService	Manual	Configurado	
Registro de eventos de Windows		EventLog	Automático	Configurado	
Registro remoto		RemoteRegistry	Deshabilitado	Configurado	
Registros y alertas de rendimiento		pla	Manual	Configurado	
Servicio Asistente para la compatibilidad de programas		PcaSvc	Automático	Configurado	
Servicio biométrico de Windows		WbioSrvc	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de actualizaciones Orchestrator para Windows Update		UsoSvc	Manual	Configurado	
Servicio de administración de		EntAppSvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
aplicaciones de empresa					
Servicio de administración de radio		RmSvc	Manual	Configurado	
Servicio de administrador de licencias de Windows		LicenseManager	Manual	Configurado	
Servicio de almacenamiento		StorSvc	Manual	Configurado	
Servicio de asociación de dispositivos		DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows		FontCache	Deshabilitado	Configurado	
Servicio de cierre de invitado de Hyper-V		vmicshutdown	Manual	Configurado	
Servicio de compatibilidad con Bluetooth		bthserv	Manual	Configurado	
Servicio de configuración de red		NetSetupSvc	Manual	Configurado	
Servicio de datos del sensor		SensorDataService	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP		WinHttpAutoProxySvc	Manual	Configurado	
Servicio de directivas de diagnóstico		DPS	Deshabilitado	Configurado	
Servicio de dispositivo de interfaz humana		hidserv	Manual	Configurado	
Servicio de enrutador de AllJoyn		AJRouter	Deshabilitado	Configurado	
Servicio de enumeración de dispositivos de tarjeta inteligente		ScDeviceEnum	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de geolocalización		lfsvc	Manual	Configurado	
Servicio de host HV		HvHost	Manual	Configurado	
Servicio de implementación de AppX (AppXSVC)		AppXSvc	Manual	Configurado	
Servicio de infraestructura de		BrokerInfrastructure	Automático	Configurado	

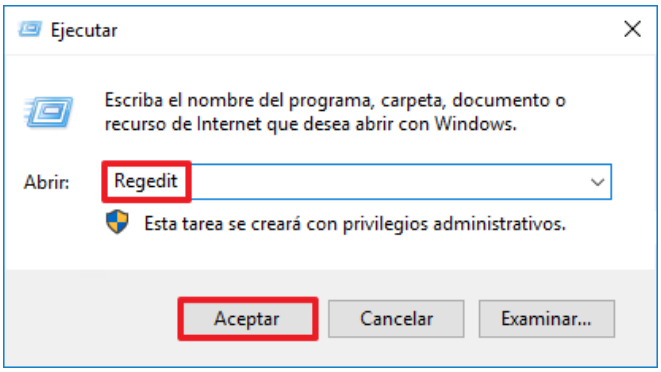
Comprobación	OK/NOK	Cómo hacerlo			
tareas en segundo plano					
Servicio de inscripción de administración de dispositivos		DmEnrollmentSvc	Manual	Configurado	
Servicio de inspección de red de Windows Defender		WdNisSvc	Manual	Configurado	
Servicio de instalación de dispositivos		DeviceInstall	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V		vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V		vmicheartbeat	Manual	Configurado	
Servicio de licencia de cliente (ClipSVC)		ClipSVC	Manual	Configurado	
Servicio de lista de redes		netprofm	Manual	Configurado	
Servicio de notificación de eventos de sistema		SENS	Automático	Configurado	
Servicio de Panel de escritura a mano y teclado táctil		TabletInputService	Deshabilitado	Configurado	
Servicio de perfil de usuario		ProfSvc	Automático	Configurado	
Servicio de plataforma de dispositivos conectados		CDPSvc	Automático	Configurado	
Servicio de protocolo de túnel de sockets seguros		SstpSvc	Manual	Configurado	
Servicio de puerta de enlace de nivel de aplicación		ALG	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de registro de acceso de usuarios		UALSVC	Automático	Configurado	
Servicio de repositorio de estado		StateRepository	Manual	Configurado	
Servicio de sensores		SensorService	Manual	Configurado	
Servicio de servidor proxy KDC (KPS)		KPSSVC	Manual	Configurado	
Servicio de sincronización de hora de Hyper-V		vmictimesync	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio de supervisión de licencias de Windows	WLMS	Automático	Configurado	
Servicio de supervisión de sensores	SensrSvc	Manual	Configurado	
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Manual	Configurado	
Servicio de uso compartido de datos	DsSvc	Manual	Configurado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Deshabilitado	Configurado	
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Manual	Configurado	
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual	Configurado	
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado	
Servicio de Windows Defender	WinDefend	Automático	Configurado	
Servicio de Windows Insider	wisvc	Manual	Configurado	
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado	
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado	
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Manual	Configurado	
Servicio FrameServer de la Cámara de Windows	FrameServer	Manual	Configurado	
Servicio host de proveedor de cifrado	WEPHOSTSVC	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
de Windows					
Servicio Informe de errores de Windows		WerSvc	Deshabilitado	Configurado	
Servicio Interfaz de almacenamiento en red		nsi	Automático	Configurado	
Servicio PowerShell Direct de Hyper-V		vmicvmsession	Manual	Configurado	
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)		diagnosticshub.standardcollector.service	Manual	Configurado	
Servicio telefónico		PhoneSvc	Manual	Configurado	
Servicios de cifrado		CryptSvc	Automático	Configurado	
Servicios de Escritorio remoto		TermService	Manual	Configurado	
Servidor		LanmanServer	Automático	Configurado	
Servidor del modelo de datos del mosaico		tiledatamodelsvc	Automático	Configurado	
Sincronizar host		OneSyncSvc	Automático	Configurado	
Sistema de cifrado de archivos (EFS)		EFS	Manual	Configurado	
Sistema de eventos COM+		EventSystem	Automático	Configurado	
SMP de Espacios de almacenamiento de Microsoft		smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V		vmicvss	Manual	Configurado	
Superfetch		SysMain	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Tarjeta inteligente		SCardSvr	Deshabilitado	Configurado	
Telefonía		TapiSrv	Deshabilitado	Configurado	
Telemetría y experiencias del usuario conectado		DiagTrack	Automático	Configurado	
Temas		Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)		RpcLocator	Manual	Configurado	
WalletService		WalletService	Manual	Configurado	
Windows Driver Foundation - User-		wudfsvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
mode Driver Framework					
Windows Installer		msiserver	Manual	Configurado	
Windows Search		WSearch	Deshabilitado	Configurado	
Windows Update		wuauserv	Manual	Configurado	
SMP de Espacios de almacenamiento de Microsoft		smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V		vmicvss	Manual	Configurado	
Superfetch		SysMain	Manual	Configurado	
Tarjeta inteligente		SCardSvr	Deshabilitado	Configurado	
Telefonía		TapiSrv	Deshabilitado	Configurado	
Telemetría y experiencias del usuario conectado		DiagTrack	Automático	Configurado	
Temas		Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)		RpcLocator	Manual	Configurado	
WalletService		WalletService	Manual	Configurado	
Windows Driver Foundation - User-mode Driver Framework		wudfsvc	Manual	Configurado	
Windows Installer		msiserver	Manual	Configurado	
26. Verifique que se han asignado los permisos correctos en el sistema de archivos		Utilizando el Explorador de Windows: **"Windows+R → Explorer"** En caso de no saber dónde apunta cada una de las rutas abreviadas que se especifica, ejecute Explorer <<ruta>> donde <<ruta>> se sustituirá por la ruta abreviada. **Nota:** Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, marcándolo con el botón derecho y eligiendo la opción "Propiedades" del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá situarse en la pestaña "Seguridad". En la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios. Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados.			

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		**Usuario**	**Permiso**	**OK/NOK**
%SystemRoot%\Registration		Administrador	Control total	
		System	Control total	
		Usuario	Leer y ejecutar	
%SystemRoot%\repair		Administrador	Control total	
		System	Control total	
%SystemRoot%\security		Administrador	Control total	
		System	Control total	
SystemRoot%\system32\cacls.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\clip.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\ras		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\rasadhlp.dll		Administrador	Control total	
%SystemRoot%\system32\rasauto.dll		Administrador	Control total	
%SystemRoot%\system32\rasautou.exe		Administrador	Control total	
%SystemRoot%\system32\raschap.dll		Administrador	Control total	
%SystemRoot%\system32\rasctrnm.h		Administrador	Control total	
%SystemRoot%\system32\rasctrs.dll		Administrador	Control total	
%SystemRoot%\system32\rasctrs.ini		Administrador	Control total	
%SystemRoot%\system32\rasdial.exe		Administrador	Control total	
%SystemRoot%\system32\rasmans.dll		Administrador	Control total	
%SystemRoot%\system32\rasmontr.dll		Administrador	Control total	
%SystemRoot%\system32\rasphone.exe		Administrador	Control total	
%SystemRoot%\system32\rasppp.dll		Administrador	Control total	
%SystemRoot%\system32\rastapi.dll		Administrador	Control total	
Archivo		**Usuario**	**Permiso**	**OK/NOK**
%SystemRoot%\system32\rastls.dll		Administrador	Control total	
%SystemRoot%\system32\runonce.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\secedit.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\telnet.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\tftp.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\tracert.exe		Administrador	Control total	
		System	Control total	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>27. Verifique los valores del registro.</td><td></td><td>Compruebe los valores del registro definidos en los Controladores de Dominio que pertenezcan al grupo categorizado como categoría media siguiendo los criterios del ENS, mediante el uso del “Editor del Registro”.
“Windows+R → Regedit”
El Control de cuentas de usuario solicitará elevación de privilegios. Pulse “Sí” para continuar.
 

<table>
<tr><th>Valor del registro</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod</td><td>0</td><td></td></tr>
<tr><td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun</td><td>255</td><td></td></tr>
<tr><td>HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation</td><td>1</td><td></td></tr>
<tr><td>HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode</td><td>1</td><td></td></tr>
<tr><td>HKLM\System\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta</td><td>10</td><td></td></tr>
<tr><td>HKLM\System\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog</td><td>1</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Valor del registro	Valor	OK/NOK
		HKLM\System\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog	20000	
		HKLM\System\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog	20	
		HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel	90	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect	0	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime	300000	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery	0	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect	1	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions	2	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions	3	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TCPMaxPortsExhausted	5	

ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.4.1. GUÍA PASO A PASO CONTROLADOR DE DOMINIO QUE LE SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se emplee Windows Server 2016, con una categorización de seguridad alta, según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar la categoría de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para los servicios e información manejada por la organización correspondieran, al menos, a la categoría alta para alguno de ellos, deberá realizar las implementaciones según se referencian en el presente anexo.

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

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

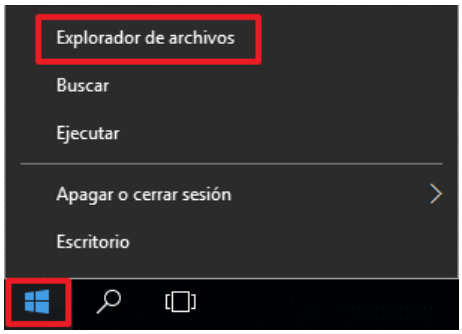
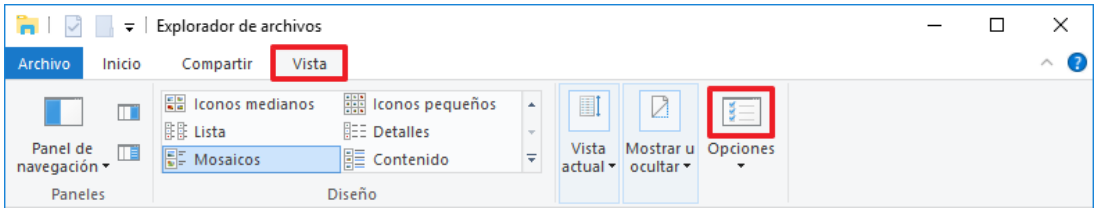
Se debe tener en cuenta que la política global definirá, a través del análisis de cada una de sus dimensiones de seguridad, el nivel de la organización. No obstante, pudiera ser factible que alguno de los servidores proporcionara servicios o gestionara información sujeta a categoría básica o media. Por lo tanto, a estos servidores les podrían ser de aplicación las plantillas de seguridad aplicables a categoría básica establecidas en el ANEXO A.2. de la presente guía o en el ANEXO A.3, si correspondiera a la categoría media. Deberá seguir, para ello, los pasos establecidos para la generación y aplicación de objetos de políticas de grupos para servidores miembros definidos en los puntos 1 y 3 de los anexos previos. Sin embargo, la política de dominio y controladores de dominio, al ser de ámbito general, deberá especificar la correspondiente a esta categoría alta siguiendo las pautas establecidas en los pasos posteriores.

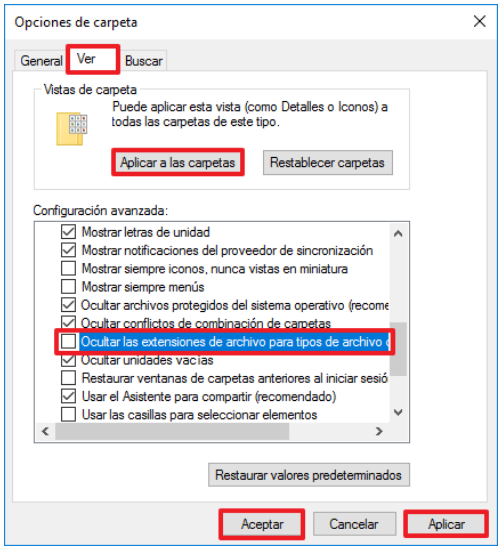
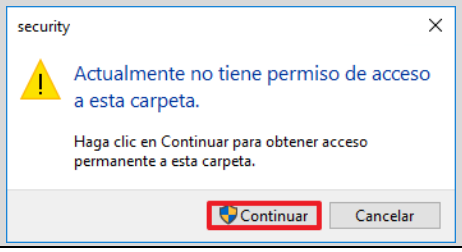
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar las pruebas de funcionalidad oportunas.

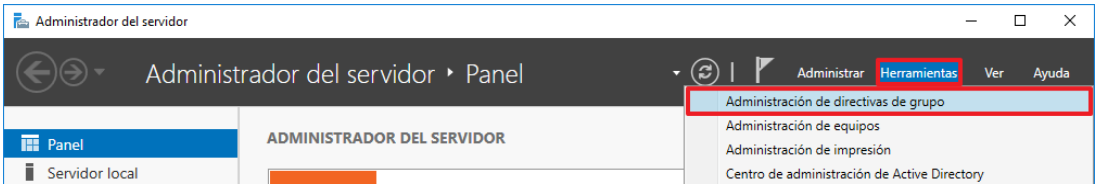
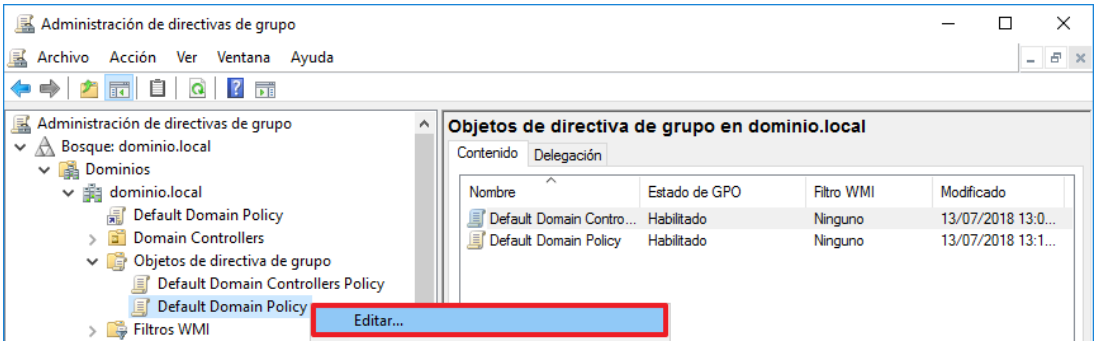
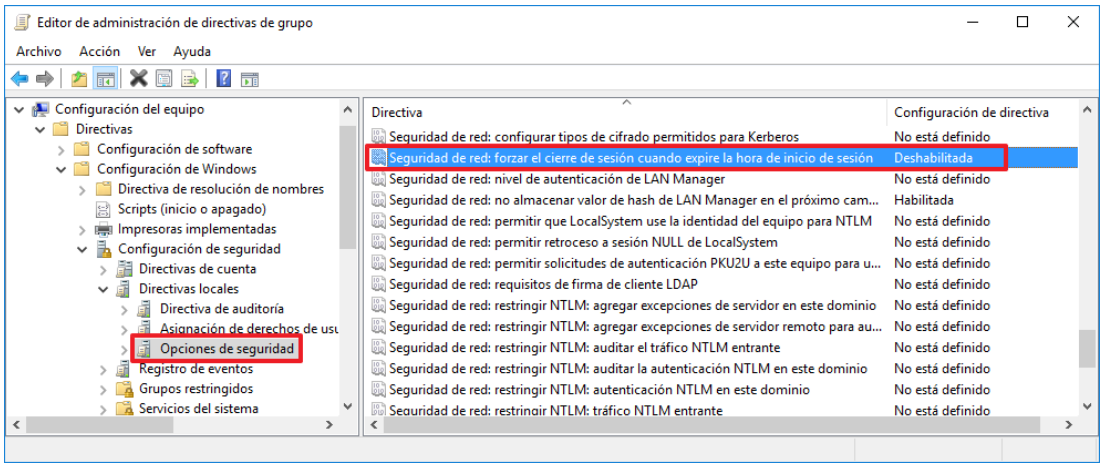
1. PREPARACIÓN DE DOMINIO

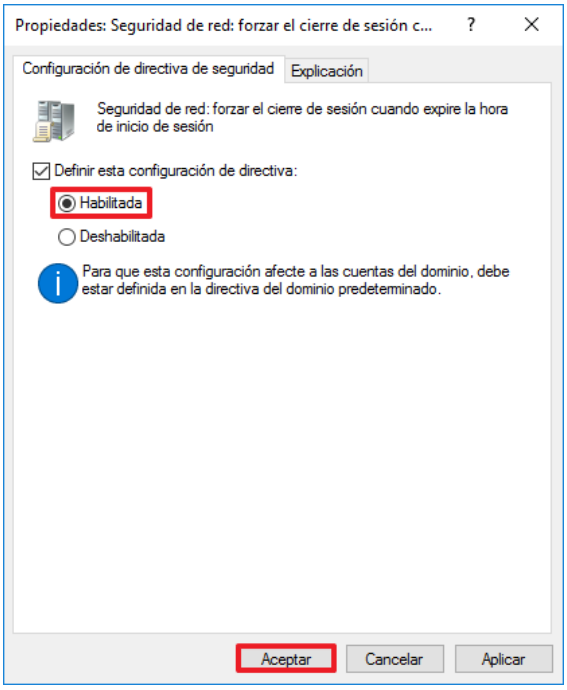
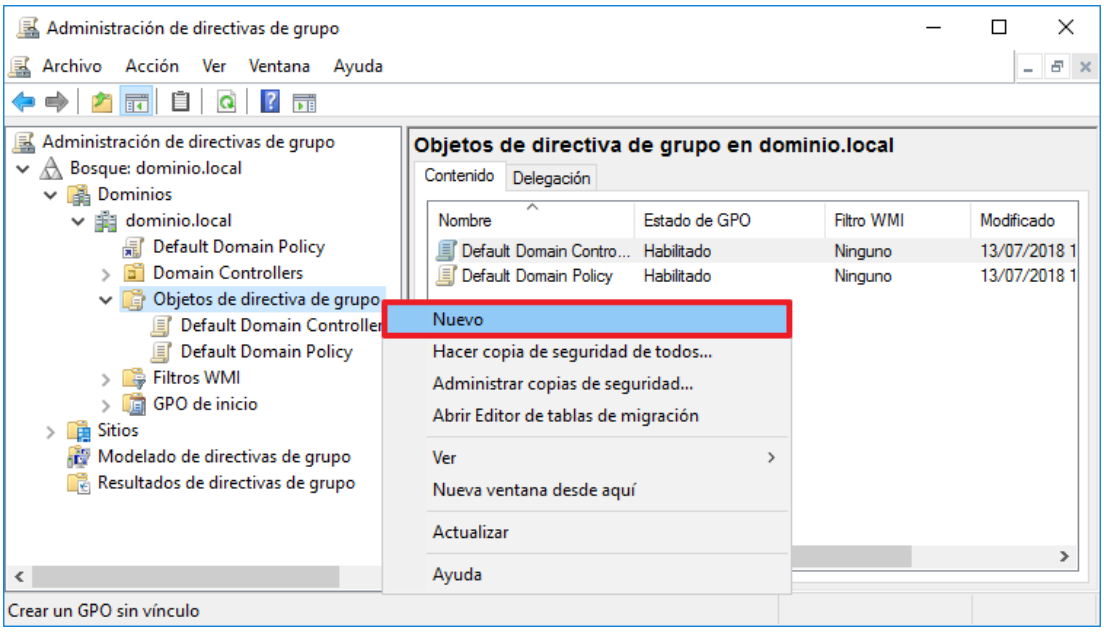
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se realizará la implementación de las plantillas de seguridad. Solo es necesario realizar este procedimiento una vez.

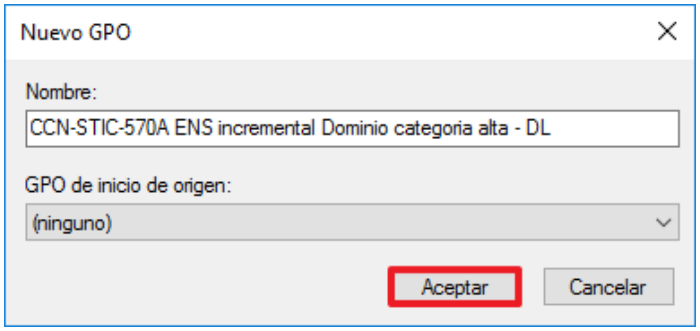
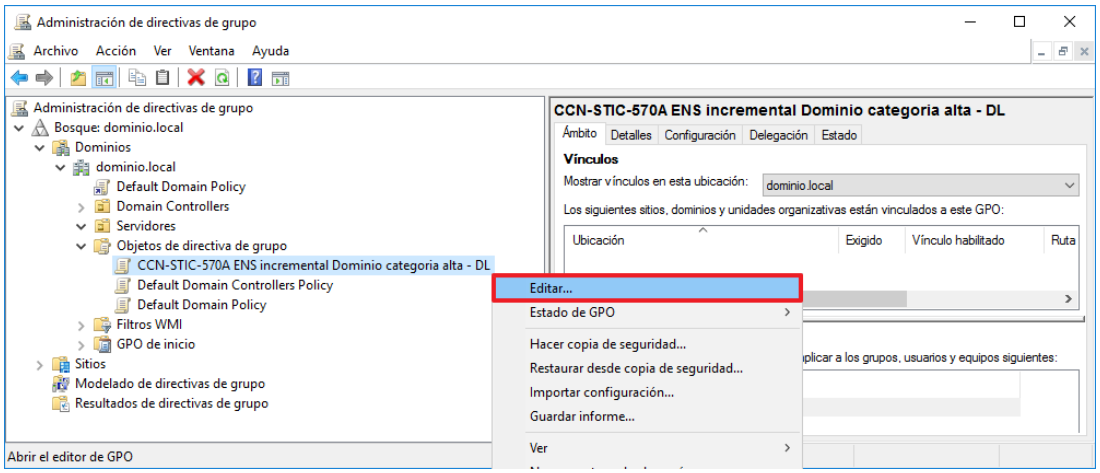
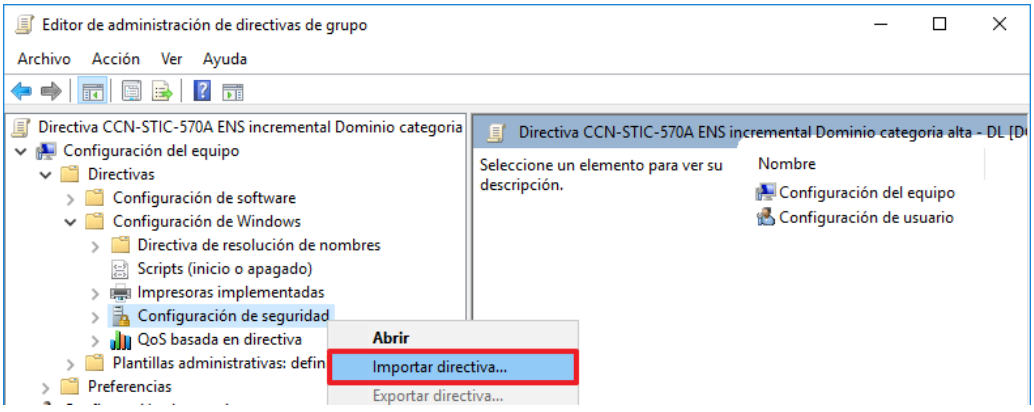
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.

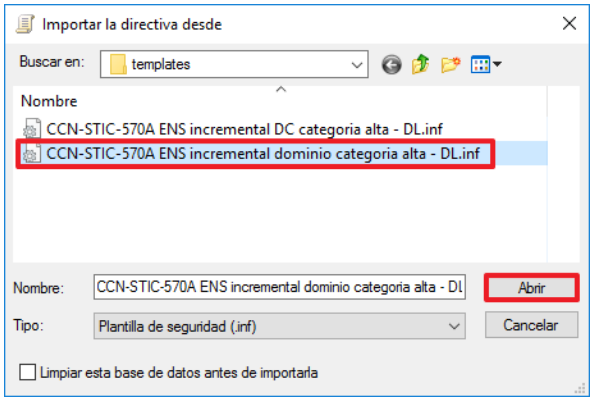
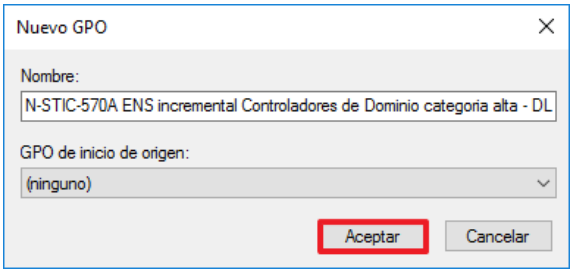
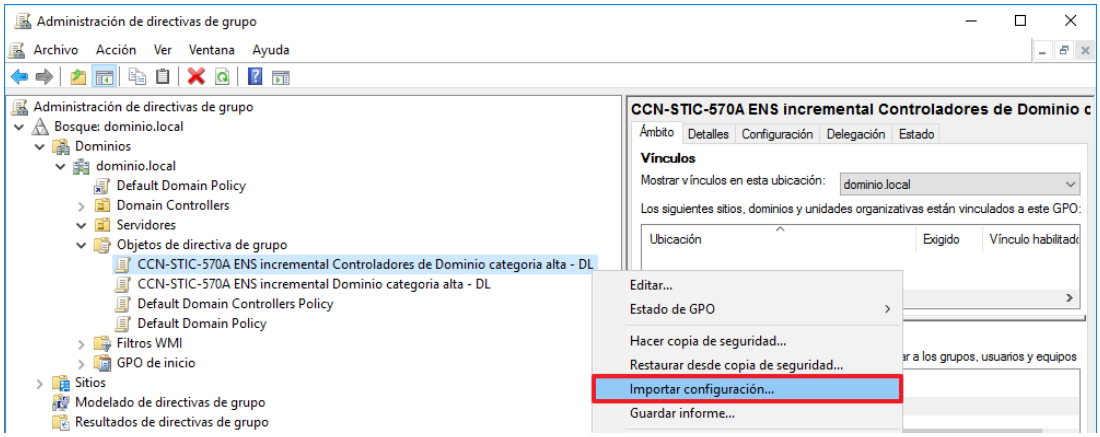
Paso	Descripción
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Cree el directorio “Scripts” en la unidad C:\.
4.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts". **Nota:** Los recursos asociados a esta guía se encuentran en el directorio “Scripts-570A”.
5.	Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de “Inicio” con el botón derecho y seleccione “Explorador de archivos”. 
6.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”. 

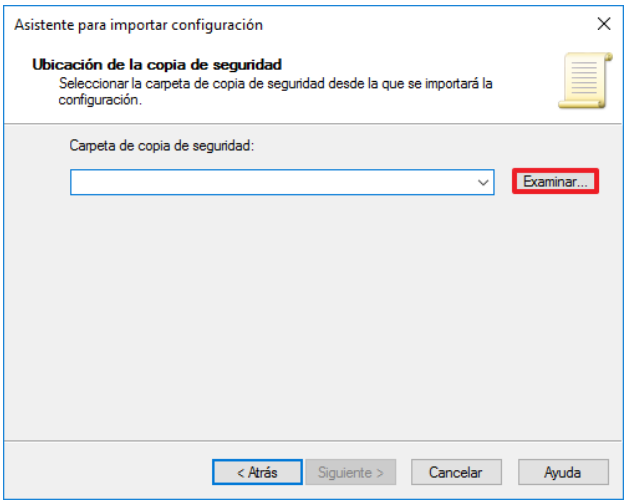
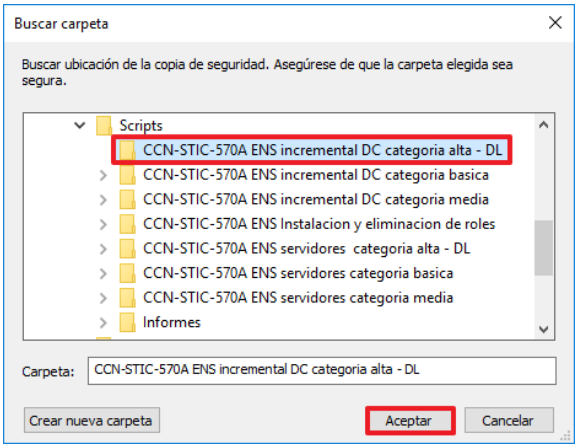
Paso	Descripción
7.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 
8.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio: – CCN-STIC-570A ENS incremental DC categoria alta - DL (directorio) – CCN-STIC-570A ENS servidores categoria alta - DL (directorio) – CCN-STIC-570A ENS incremental DC categoria alta - DL.inf – CCN-STIC-570A ENS incremental dominio categoria alta - DL.inf – CCN-STIC-570A ENS Incremental servidores categoria alta - DL.inf
9.	Copie los ficheros “CCN-STIC-570A ENS incremental dominio categoria alta - DL.inf” y “CCN-STIC-570A ENS incremental DC categoria alta - DL.inf, al directorio “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Según la configuración de seguridad de UAC, el sistema podría solicitar la elevación de privilegios, en este caso, pulse “Continuar”. 

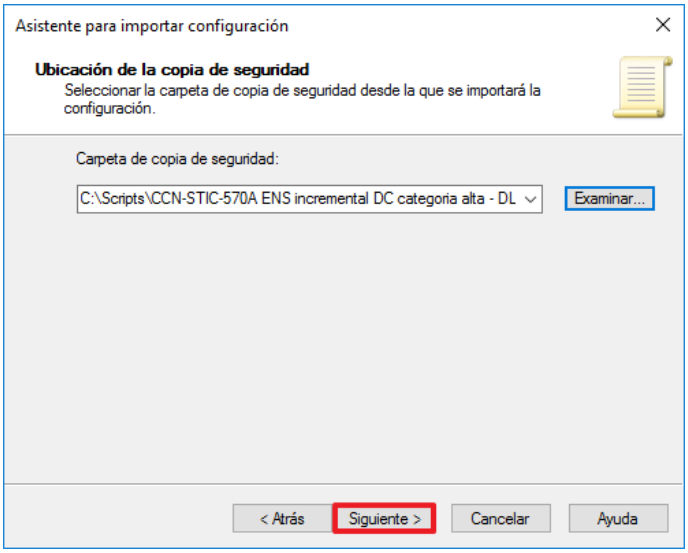
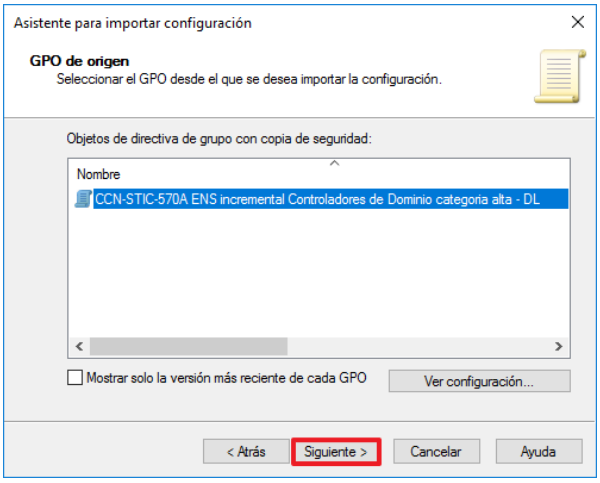
Paso	Descripción
10.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”** 
11.	Despliegue los contenedores y pulse doble clic sobre la carpeta “Objetos de directiva de grupo”.
12.	Sitúese sobre el objeto “Default Domain Policy” y haga clic derecho con el ratón. Seleccione “Editar” en el menú contextual que se ha desplegado. 
13.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”** Pulse doble clic sobre la directiva “Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión”. 

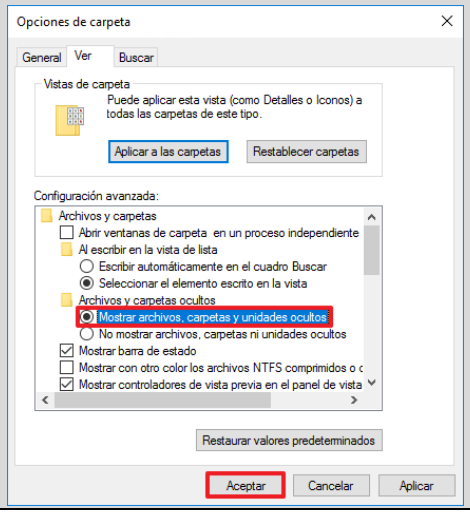
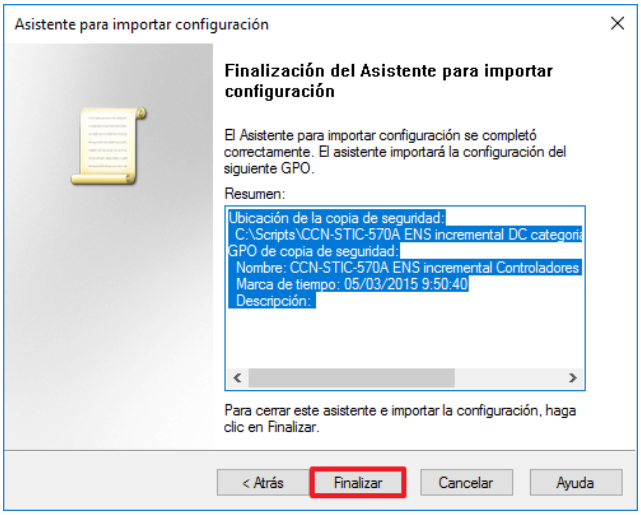
Paso	Descripción
14.	En el menú de propiedades de la directiva, seleccione la opción “Habilitada” y pulse sobre “Aceptar”. 
15.	Cierre el “Editor de administración de directivas de grupo”.
16.	De nuevo, en la consola de administración de directivas de grupo despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”.
17.	Pulse con el botón derecho, sobre dicha y carpeta y seleccione la opción “Nuevo”. 

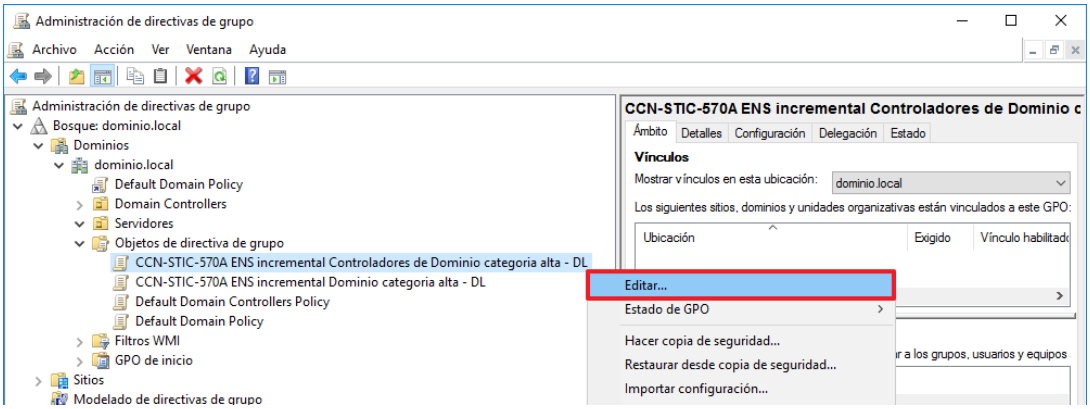
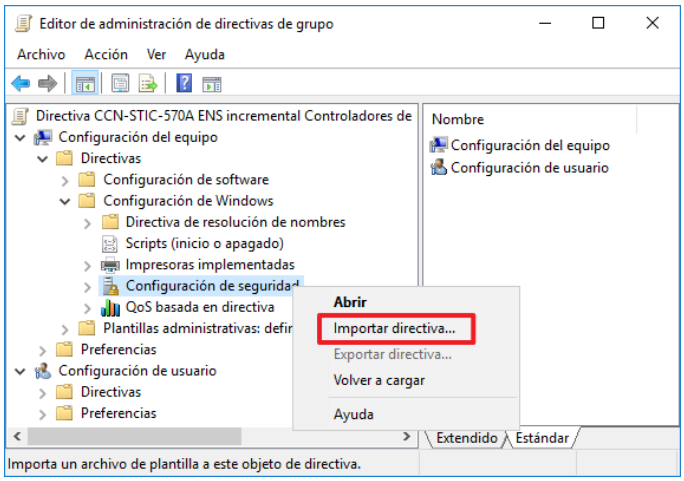
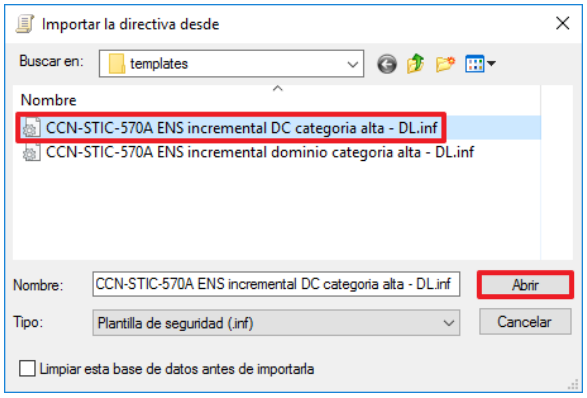
Paso	Descripción
18.	Introduzca como nombre “CCN-STIC-570A ENS incremental Dominio categoria alta - DL” y pulse el botón “Aceptar”. 
19.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
20.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**
21.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva…”. 

Paso	Descripción
22.	Seleccione de la ruta “C:\Windows\Security\Templates” el fichero “CCN-STIC-570A ENS incremental Dominio categoria alta - DL” y pulse el botón “Abrir”. 
23.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
24.	Vuelva a pulsar con el botón derecho sobre el contenedor de objetos de directiva de grupo y seleccione la opción “Nuevo”.
25.	Introduzca como nombre “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL” y pulse el botón “Aceptar”. 
26.	La nueva política requiere una configuración de plantillas administrativas. Para ello y seleccionando la política, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración…”. 
27.	En el asistente de importación de configuración, pulse el botón “Siguiente >”.

Paso	Descripción
28.	En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.
29.	En “Carpeta de copia de seguridad”, pulse el botón “Examinar...”. 
30.	Seleccione la carpeta “CCN-STIC-570A ENS incremental DC categoria alta - DL” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 

Paso	Descripción
31.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada. 
32.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-570A incremental DC categoria alta - DL” y pulse el botón “Siguiente >”. 

Paso	Descripción
	Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero "manifest.xml". Este es un fichero oculto y, por lo tanto, debe mostrar en "opciones de carpeta" la opción "Mostrar archivos, carpetas y unidades ocultos". 
33.	En la pantalla de examen, pulse el botón "Siguiente >".
34.	Para completar el asistente pulse el botón "Finalizar". 
35.	Pulse el botón "Aceptar" para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración.

Paso	Descripción
36.	A continuación, seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
37.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**
38.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva…”. 
39.	Seleccione de la ruta “C:\Windows\Security\Templates” el fichero “CCN-STIC-570A ENS incremental DC categoria alta - DL” y pulse el botón “Abrir”. 

Paso	Descripción
40.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
41.	Las políticas se encuentran ya creadas correctamente. No obstante, no se aplicarán hasta más adelante, una vez que haya tenido en cuenta y aplicado todas las consideraciones adicionales que se mostrarán en el siguiente punto del presente anexo. Cierre la herramienta “Administración de Directivas de Grupo”.

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

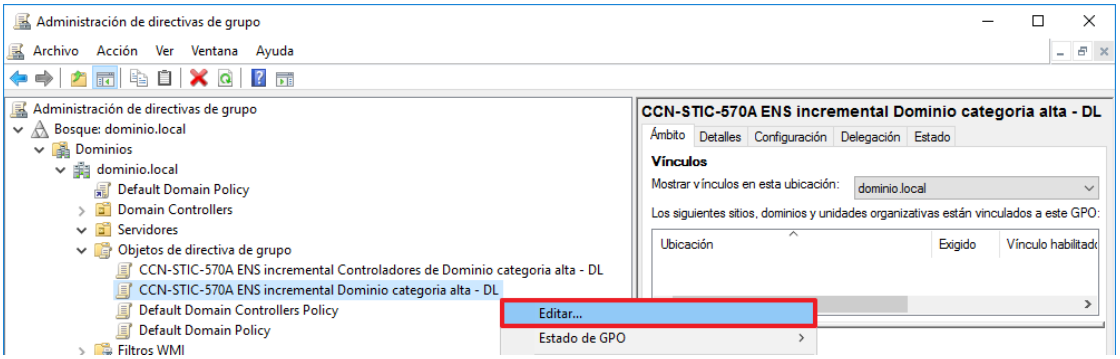
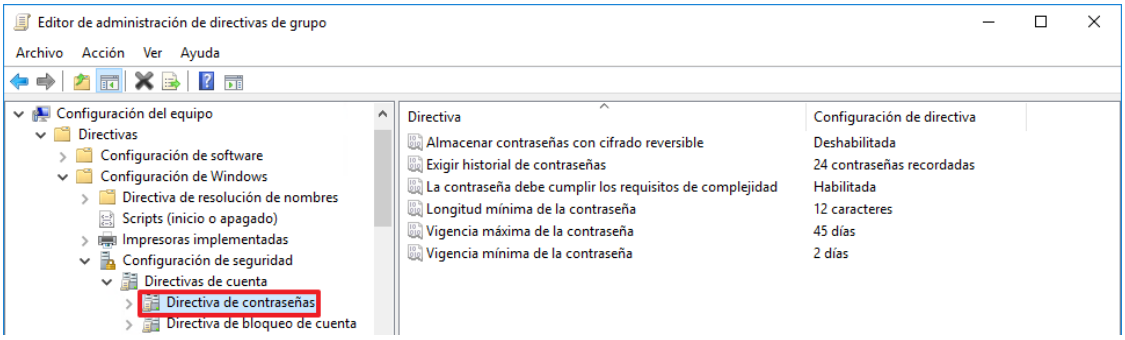
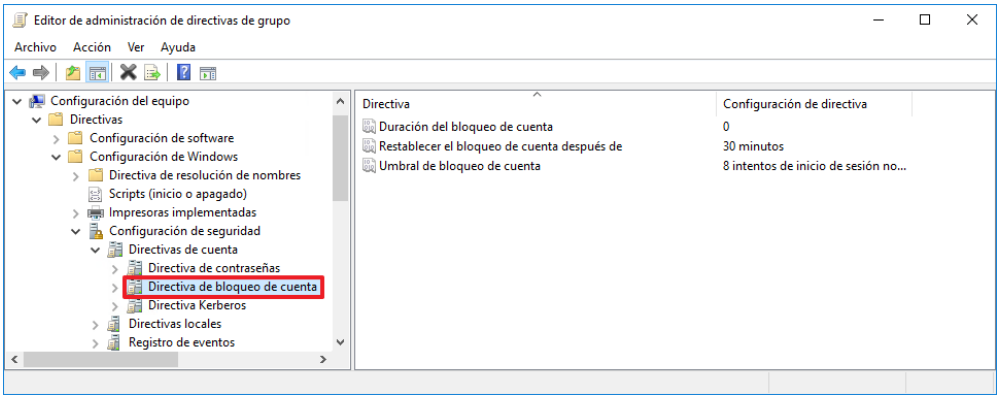
El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración. Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría alta. No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

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

2.1. CONTRASEÑAS Y BLOQUEO DE CUENTAS

Es factible que su organización cuente con una política de contraseña consolidada. La implementación de la política que se aplicará sobre el dominio "CCN-STIC-570A ENS incremental Dominio categoria alta - DL" aplicará una de forma particular. Deberá evaluarla para determinar si esta configuración le es válida o por el contrario debe adaptarla a las condiciones de su organización.

Paso	Descripción
42.	Para evaluar y realizar la modificación oportuna inicie la herramienta "Administración de Directivas de Grupo". Para ello y sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"** 

Paso	Descripción
43.	Edite el objeto de GPO “CCN-STIC-570A ENS incremental Dominio categoria alta - DL”. Para ello seleccione dicha política y seleccione la opción “Editar…”. 
44.	Despliegue la política y sitúese en la siguiente ruta: **“Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseñas”** 
45.	Evalúe la política de contraseñas y modifíquela convenientemente. **Nota:** Debe tener en consideración que si su política de credenciales es menos rigurosa que la marcada en la configuración deseada, se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de contraseñas a lo marcado por la configuración recomendada.
46.	De forma similar a lo anterior, deberá evaluar la política de bloqueo de cuenta. Para ello y sin cerrar la política, seleccione la “Directiva de bloqueo de cuenta” que encontrará al mismo nivel que la directiva de contraseña. 

Paso	Descripción
47.	Evalúe la política de bloqueo de cuenta y modifíquela convenientemente. **Nota:** Debe tener en consideración que si su política de bloqueo de cuenta es menos rigurosa que la marcada en la configuración deseada, se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de bloqueo de cuenta a lo marcado por la configuración recomendada.
48.	Cierre el "Editor de administración de directivas de grupo".
49.	Cierre la herramienta "Administración de directivas de grupo".

2.2. INFORMACIÓN DE OBLIGACIONES

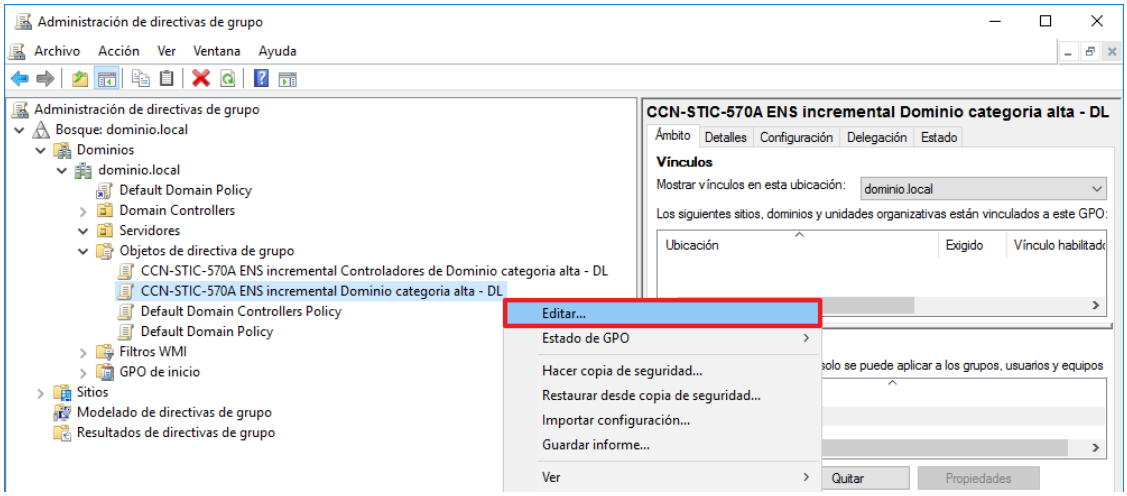
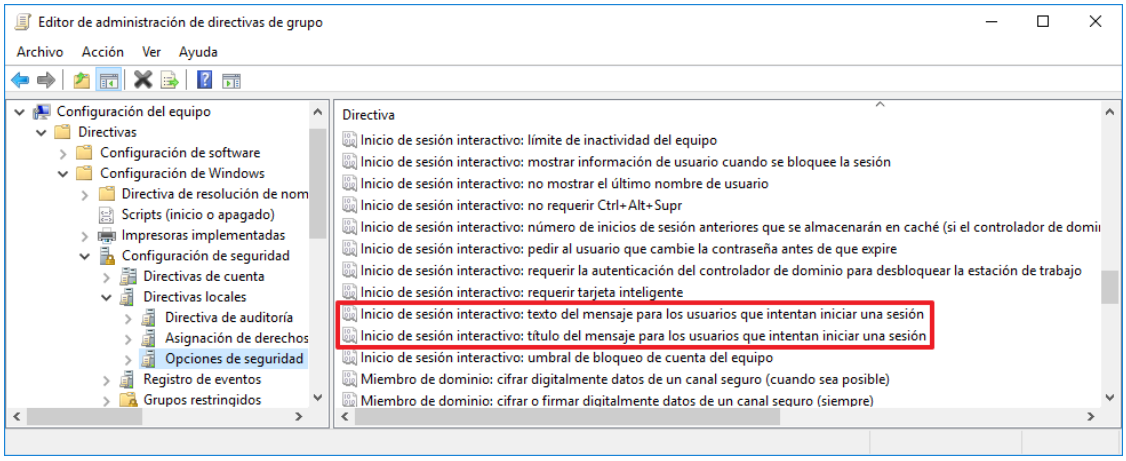
Uno de los aspectos que marca el ENS desde su requisito de categoría básica en el Marco Operacional para el acceso local, consiste en la necesidad de informar al usuario de sus obligaciones.

Los sistemas Windows presentan mecanismos para implementar mensajes que realizan advertencias al usuario cuando va a realizar el inicio de la sesión. Aunque pudieran emplearse otros tales como la ejecución de scripts, el empleo de este mecanismo es altamente recomendable. Debe, no obstante, tomarse en consideración que su organización ya está empleando este mecanismo para notificar otros detalles como los marcados por el Reglamento Europeo General de Protección de Datos (GDPR) 2016/679/CE y la Ley Orgánica 15/1999 de protección de datos de carácter personal.

Si fuera así, modifique el mensaje mostrado para adaptarlo también al cumplimiento del ENS según lo estipulado en la política de seguridad de su organización.

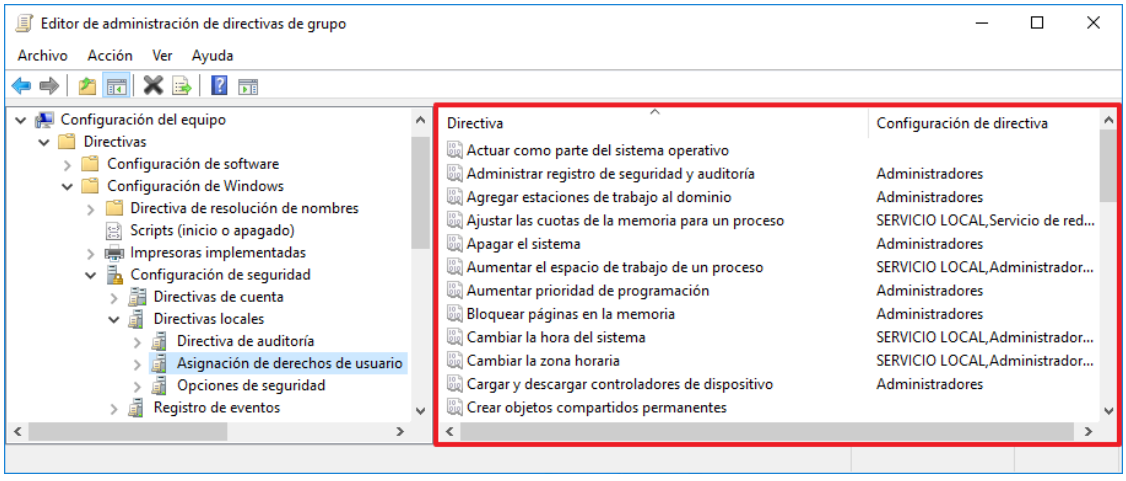
Si su organización no está haciendo uso de este mecanismo siga los siguientes pasos para habilitar el sistema de advertencia, con objeto de informar al usuario de sus obligaciones, según quede estipulado en la política de seguridad de la organización.

Paso	Descripción
50.	Inicie la herramienta "Administración de Directivas de Grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"** 

Paso	Descripción
51.	Edite el objeto de GPO “CCN-STIC-570A ENS incremental Dominio categoria alta - DL”. Para ello seleccione dicha política y seleccione la opción “Editar…”. 
52.	Despliegue la política y sitúese en la siguiente ruta: **“Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**
53.	Identifique las directivas “Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión” e “Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión”. 
54.	Edite ambas directivas incluyendo el título de la advertencia y el mensaje a facilitar a los usuarios según se estipule en las políticas de seguridad de la organización.
55.	Cierre la política de seguridad.
56.	Cierre “Administración de Directivas de Grupo”.

2.3. ASIGNACIÓN DE DERECHOS DE USUARIO

Paso	Descripción

Paso	Descripción
57.	Los objetos de políticas de grupo para Controladores de Dominio y Servidores miembros especifican unos derechos de usuario siguiendo planteamientos de seguridad que aplican los principios de mínimo privilegio y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les hayan asignado derechos determinados para la administración o gestión de los sistemas. Si esto fuera así, deberá realizar las modificaciones pertinentes sobre el objeto de política de grupo "CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL".
58.	Edite la política de grupo correspondiente iniciando la herramienta "Administración de Directivas de Grupo" y seleccionando la política a modificar. Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"** Sobre el objeto de GPO que se quiere modificar, deberá pulsar clic derecho y seleccionar "Editar" en el menú desplegado.
59.	Una vez abierto el "Editor de administración de directivas de grupo", despliegue la política y sitúese en la siguiente ruta: **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"** 
60.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
61.	Guarde la configuración cerrando la ventana de editor de administración de directivas de grupo.

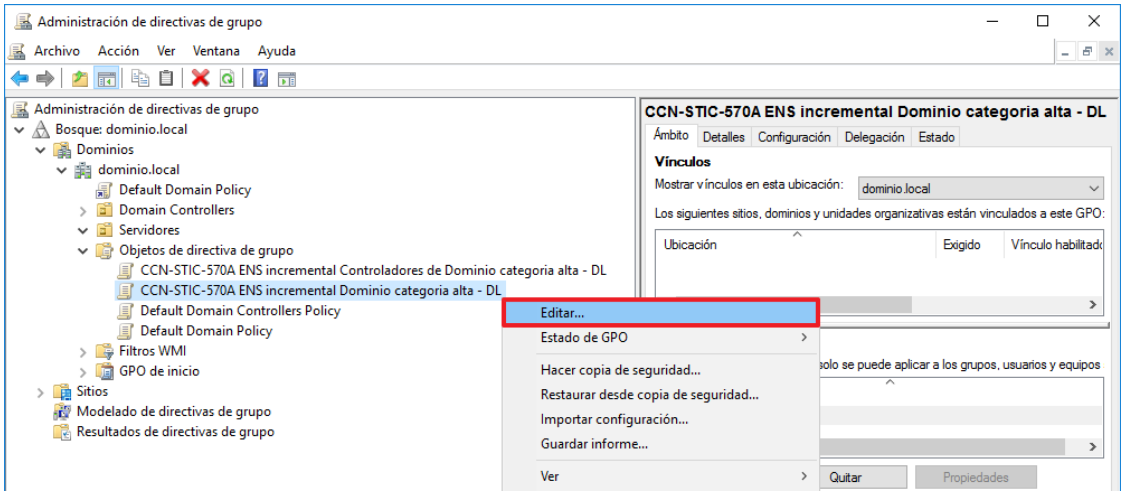
2.4. BLOQUEO DE SESIÓN ANTE INACTIVIDAD

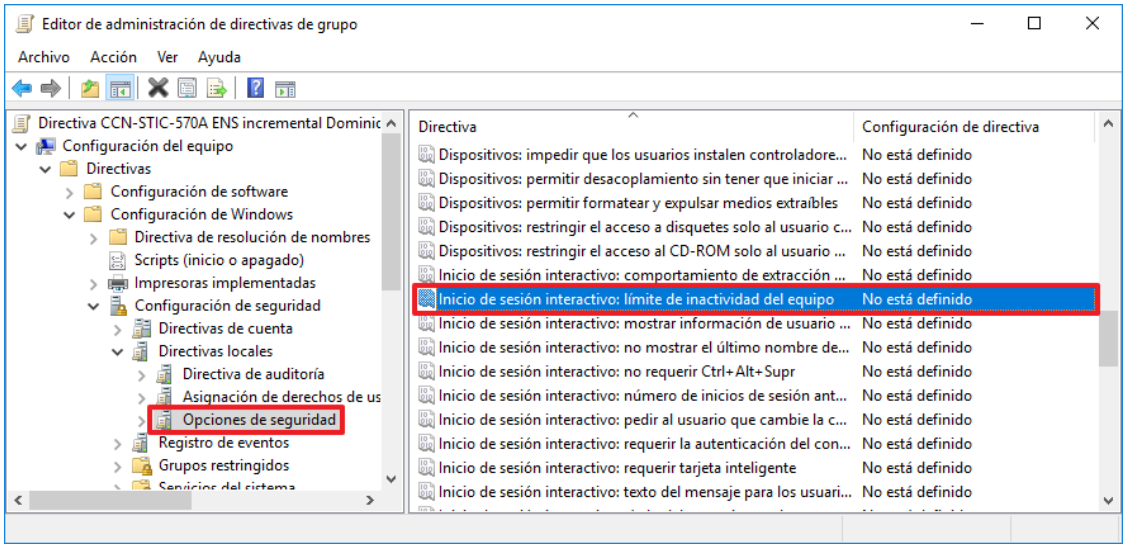
Se establece, a partir de la categoría media y según MP. EQ. 2, la necesidad de realizar el bloqueo del equipo ante un tiempo razonable de inactividad. A través de las políticas de grupo aplicables sobre el usuario, puede establecerse la medida de protección que habilita el salvapantallas y, por lo tanto, el bloqueo de la sesión.

La implementación de esta medida puede realizarse a través de estrategias diferentes. La presente guía determina la aplicación a todo el dominio modificando la política de dominio. No obstante, también podría determinarse crear una política nueva que, aplicable a nivel del dominio, solo fuera efectiva a un grupo de usuarios concretos.

Debe tener en consideración que la política de bloqueo por salvapantallas se aplica a través de GPO por usuario y no por equipo.

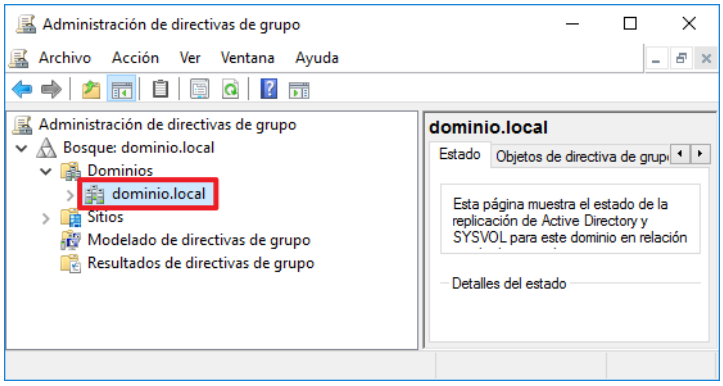
Si la organización presenta mecanismos para realizar el bloqueo del equipo ante inactividad no es necesario que aplique la siguiente configuración. No obstante, revise la configuración para adaptarse a la normativa vigente. Si la organización no tiene medidas dispuestas siga los siguientes pasos.

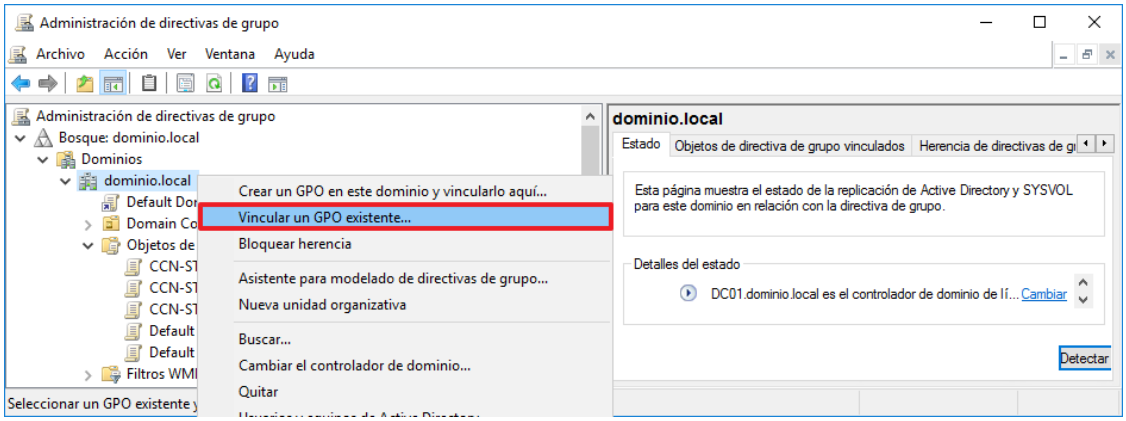
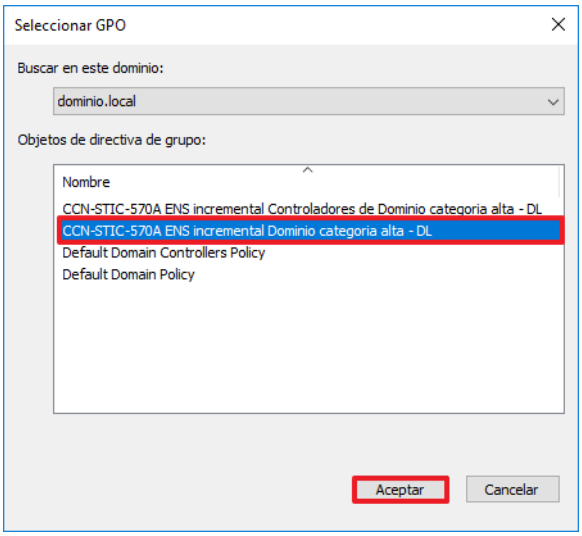
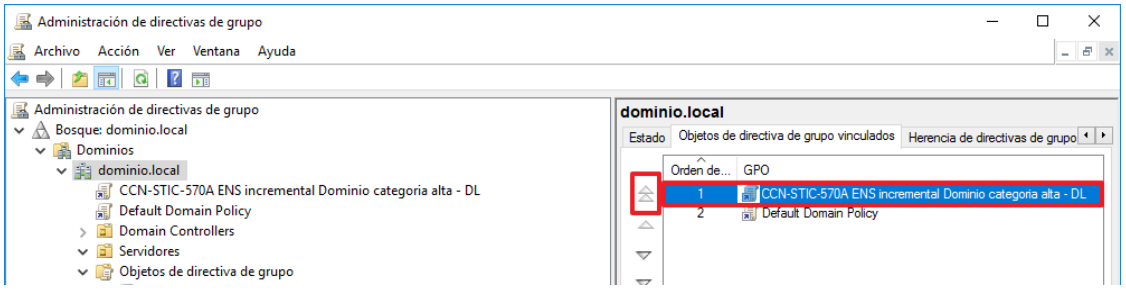
Paso	Descripción
62.	Para evaluar y realizar la modificación oportuna inicie la herramienta “Administración de directivas de grupo”.
63.	Edite el objeto de GPO “CCN-STIC-570A ENS incremental Dominio categoria alta - DL”. Para ello seleccione dicha política y seleccione la opción “Editar…”. 

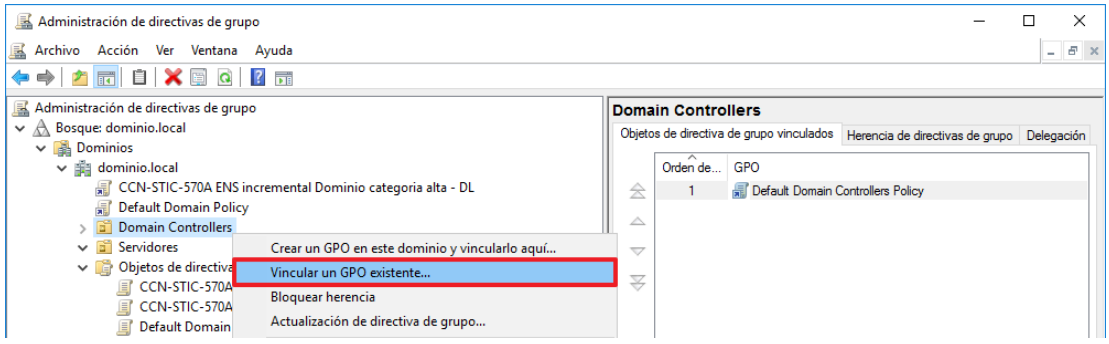
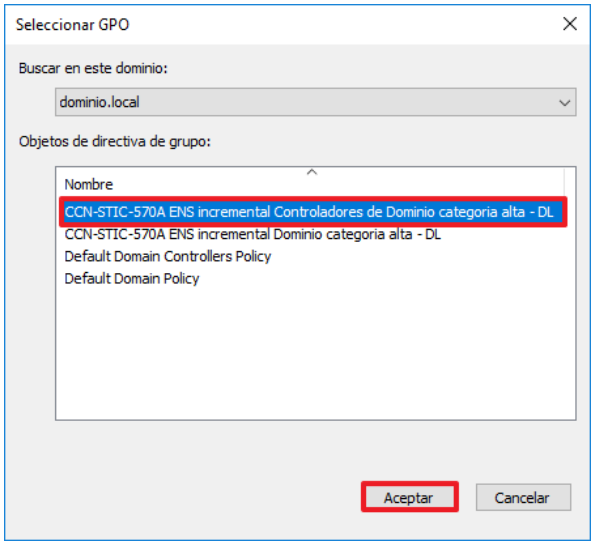
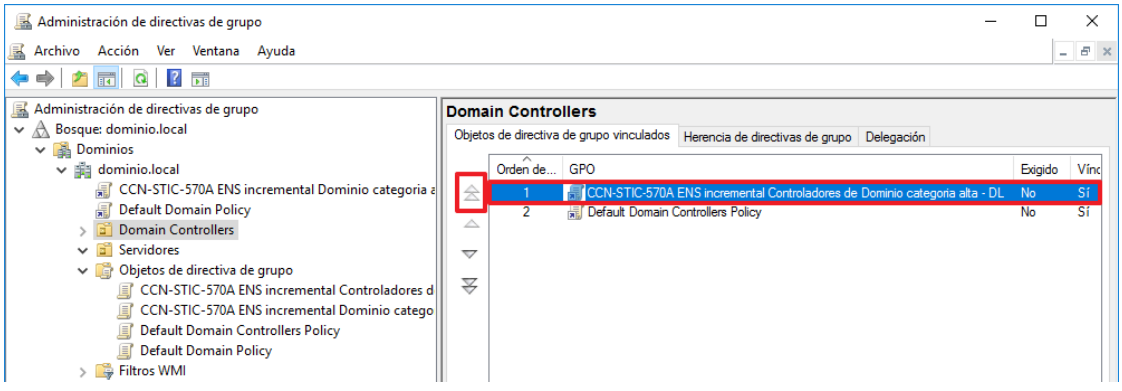
Paso	Descripción
64.	Despliegue la política y sitúese en la siguiente ruta: **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"** Habilite y configure la directiva de seguridad: – Inicio de sesión interactivo: límite de inactividad del equipo Establezca el valor en 600 segundos (10 minutos). 
65.	Cierre la política.

3. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

El presente punto establece la aplicación de las políticas de seguridad, toda vez que se han tenido en consideración las condiciones definidas en el punto previo.

Paso	Descripción
66.	Inicie la herramienta de administración de directivas de grupo.
67.	Despliegue el bloque y posiciónese sobre su dominio.  **Nota:** En el ejemplo el dominio utilizado se denomina "dominio.local".

Paso	Descripción
68.	Pulse con el botón derecho sobre el mismo y seleccione la opción “Vincular un GPO existente…”. 
69.	Seleccione la política “CCN-STIC-570A ENS incremental Dominio categoria alta - DL” y pulse el botón “Aceptar”. 
70.	Una vez agregado, en el panel derecho seleccione la pestaña “Objetos de directiva de grupo vinculados” y seleccione la política “CCN-STIC 570A ENS incremental Dominio categoria alta - DL”.
71.	Pulse el botón con la flecha que apunta hacia arriba hasta situar la política “CCN-STIC 570A ENS incremental Dominio categoria alta - DL” en primer lugar dentro del orden de vínculo. 

Paso	Descripción
72.	Seleccione la Unidad Organizativa “Domain Controllers” y seleccione la opción “Vincular un GPO existente…”.  **Nota:** Si sus controladores de dominio se encontraran en otra ubicación vincule la siguiente GPO en dicha OU.
73.	Seleccione la política “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL” y pulse el botón “Aceptar”. 
74.	Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL” y pulse el botón con la flecha que apunta hacia arriba hasta situarla en primer lugar dentro del orden de vínculo. 

Paso	Descripción
75.	Cierre la herramienta de administración de directivas de grupo.
76.	Elimine la carpeta “C:\Scripts”.

4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD EN LOS EQUIPOS

Las configuraciones planteadas a través de la presente guía han sido ampliamente probadas en entornos de operativa Microsoft. No obstante, no se han podido probar todas las condiciones existentes, ni con las peculiaridades de cada organización. Bajo determinadas condiciones, pudieran suceder algunas incidencias que se describen a continuación, así como su resolución.

Debe tenerse en consideración que la resolución consiste en rebajar algunos de los mecanismos de seguridad descritos en la presente guía. Por lo tanto, deberá tener en consideración la problemática y ofrecer una solución que permita recuperar el estado de seguridad deseado y recomendado por la presente guía.

Un elemento significativo para los procesos de autenticación en el marco de un dominio, lo corresponde la autenticación Kerberos. El proceso de validación se realiza mediante sistemas que garantizan la confidencialidad e integridad de la información transmitida. No obstante, debe tenerse en consideración que no todos los algoritmos admitidos por Microsoft son seguros y, por lo tanto, no son compatibles con la seguridad planteada a través del Esquema Nacional de Seguridad. La política de seguridad de dominio para categorías altas presenta una implementación de mínimos adecuados con los requisitos de seguridad. No obstante, las pruebas efectuadas en laboratorio han permitido determinar que el empleo de determinados clientes o servidores Linux, o bien la integración con sistemas operativos Microsoft ya obsoletos, pudiera ser incompatible con la configuración establecida.

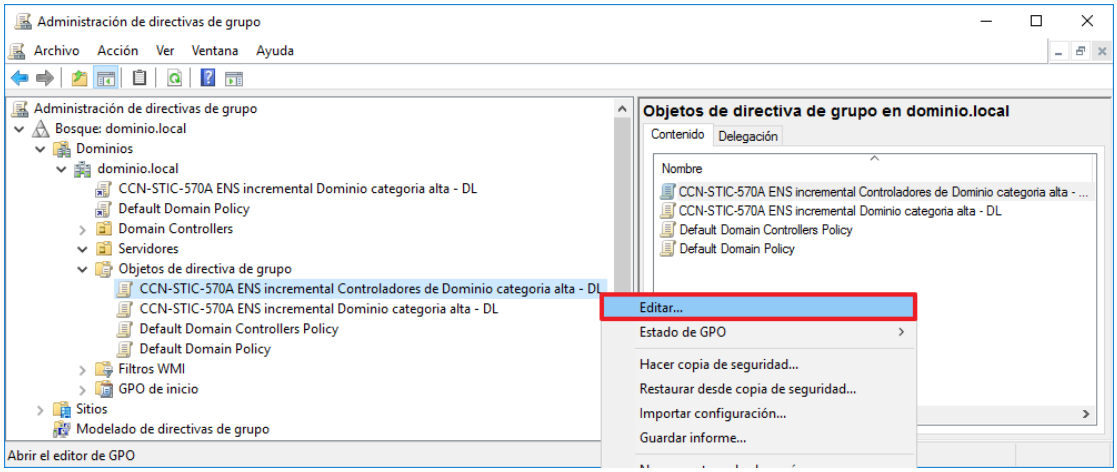
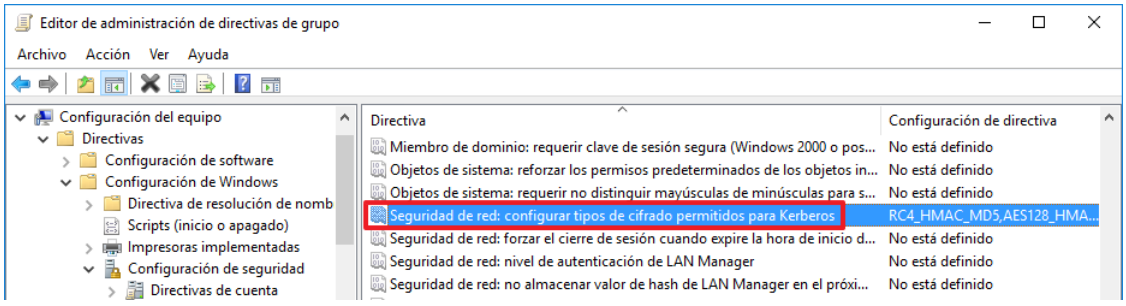
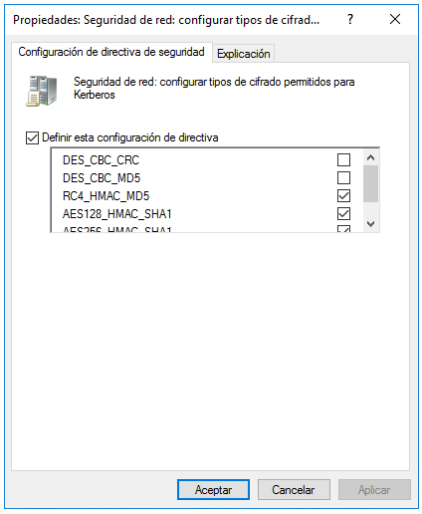
También pudieran darse problemas de comunicación ante determinadas relaciones entre diferentes árboles de un mismo bosque que han ido evolucionando desde dominios Windows NT, Windows 2000, Windows 2003 o Windows 2008.

Nota: Tenga en consideración que Windows Server 2016 ya no está soportado para trabajar a nivel funcional de Windows Server 2003, por lo que deberá actualizar su infraestructura para que el nivel funcional sea superior a 2003.

En caso de identificar problemas de validación de equipos previos a Windows XP o no Microsoft, o bien entre dominio o árboles de un mismo bosque, cuando ponga en producción la política de dominio “CCN-STIC-570A ENS incremental Dominio categoria alta - DL”, deberá realizar una modificación sobre la misma.

4.1. CIFRADOS PERMITIDOS PARA KERBEROS

Paso	Descripción
77.	Para evaluar y realizar la modificación oportuna inicie la herramienta de “Administración de directivas de grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**

Paso	Descripción
78.	Edite el objeto de GPO “CCN-STIC-570A ENS incremental Dominio categoria alta - DL”. Para ello seleccione dicha política y seleccione la opción “Editar…”. 
79.	Despliegue la política y sitúese en la siguiente ruta: **“Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**
80.	Identifique la directiva “Seguridad de red: configurar tipos de cifrado permitidos para Kerberos”. 
81.	Edítela pulsando doble clic sobre la misma. La configuración predeterminada de seguridad para el cumplimiento de ENS en su categoría alta, es la siguiente. 

Paso	Descripción
82.	Active el resto de opciones pulsando sobre los recuadros que no están marcados y cierre la política mediante el botón “Aceptar”.
83.	Aplique, a posteriori, la nueva configuración para evaluar si se han resuelto las incidencias identificadas. **Nota:** Debe tener en consideración que, si ha implementado algoritmos de seguridad alternativos a los propuestos en la configuración deseada de esta guía, se encuentra por debajo de los requerimientos de seguridad actuales. Debería evaluar a qué se deben dichas incidencias y resolverlas para volver a un estado de seguridad adecuado. Es factible que los procesos de autenticación Kerberos para determinados sistemas requieran de algoritmos débiles y pueda encontrarse ante riesgos de seguridad significativos para la organización exponiéndose, por ejemplo, a ataques de tipo *man in the middle* contra los procesos de autenticación en el dominio.

ANEXO A.4.2. LISTA DE COMPROBACIÓN DE WINDOWS SERVER 2016 COMO CONTROLADOR DE DOMINIO PARA LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía “ANEXO A.4.1 GUÍA PASO A PASO CONTROLADOR DE DOMINIO QUE LE SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS”.

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los dominios y servidores Windows Server 2016 con implementación de seguridad de categoría alta del ENS.

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

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

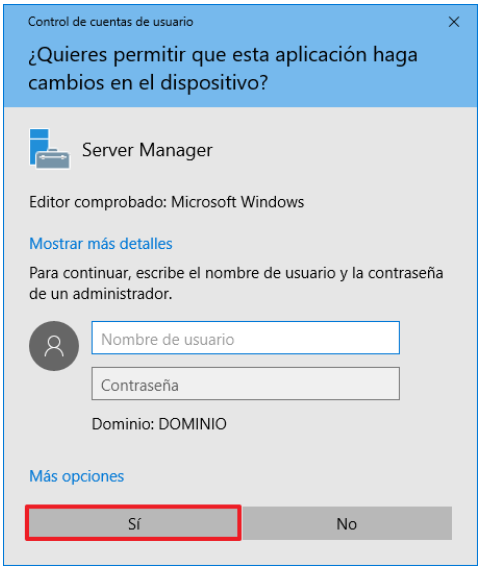
b) Conjunto resultante de directivas (rsop.msc).

c) Consola de servicios (services.msc).

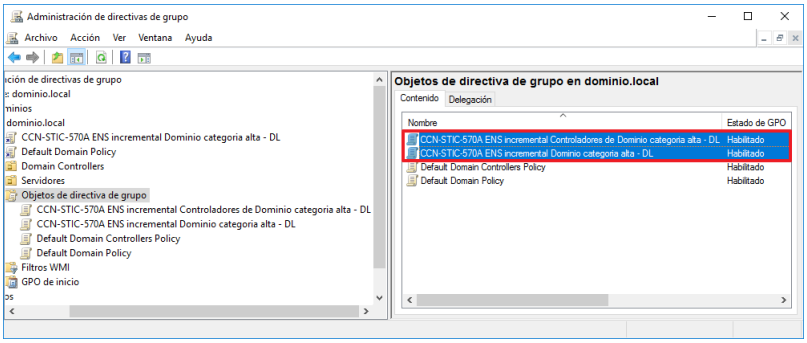
d) Editor de registro (regedit.exe).

e) Explorador de Archivos (explorer.exe).

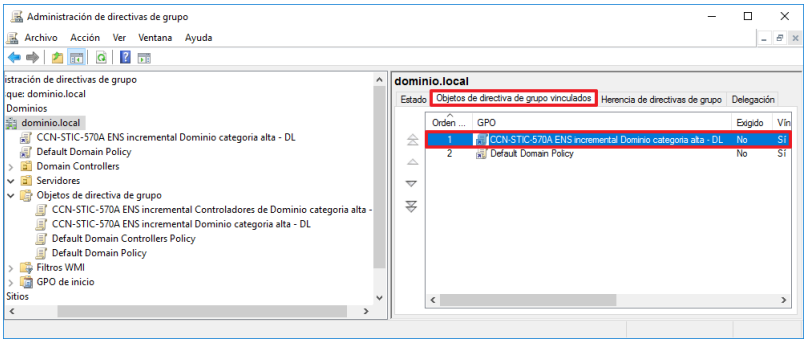
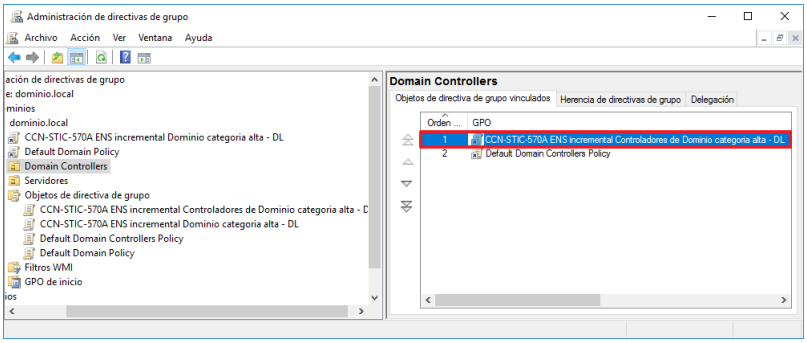
f) Usuarios y equipos de Active Directory (dsa.msc).

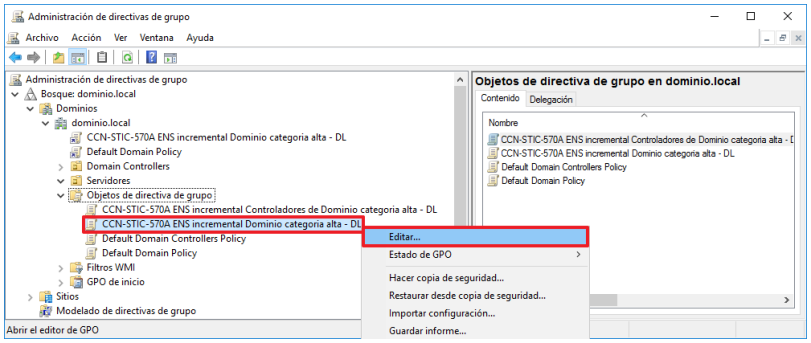
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor".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

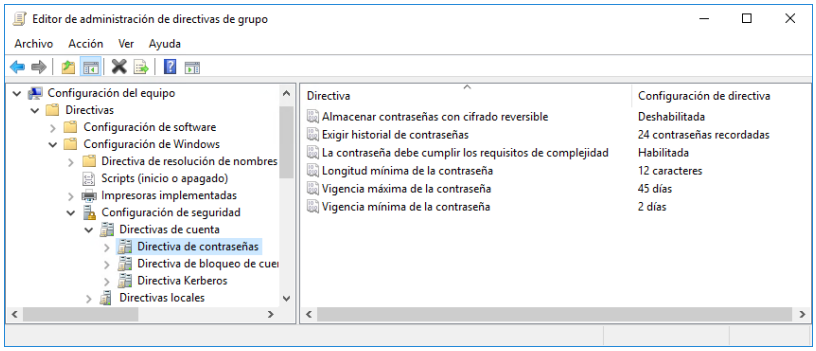
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>2. Verifique que los objetos de directivas de grupo han sido creados y están habilitados.</td><td></td><td>
Ejecute la herramienta “Administrador de directivas de grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione:
“Herramientas → Administración de directivas de grupo”


Dentro de la consola diríjase a los “Objetos de directiva de grupo”:
“Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo”
Verifique que están creados los dos objetos de directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL” y “CCN-STIC-570A ENS incremental Dominio categoria alta - DL”, y que en la columna “Estado de GPO” figuran como habilitadas.


<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL</td><td>Habilitado</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS incremental Dominio categoria alta - DL</td><td>Habilitado</td><td></td></tr>
</table>
</td></tr>
</table>

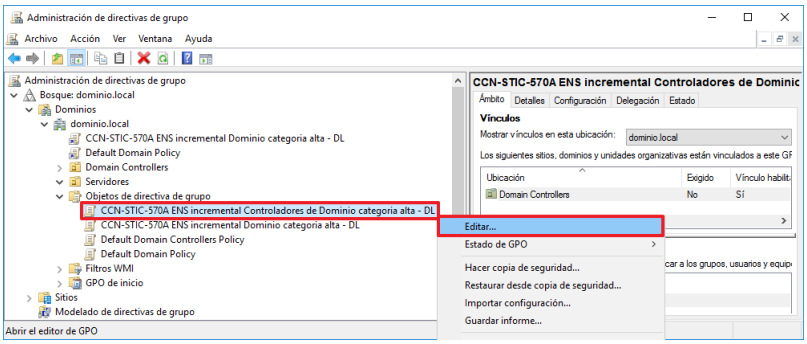
Comprobación	OK/NOK	Cómo hacerlo
3. Verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Dominio categoria alta - DL” aplica a todos los objetos del dominio y ocupa el primer lugar en el orden de vinculación.		En el árbol de la izquierda sitúese sobre el dominio desde: **“Bosque: [Su Bosque] → Dominios → [Su Dominio]”** En la pestaña “Objetos de Directiva de grupo vinculados” verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Dominio categoria alta - DL” figura en el panel de la derecha y ocupa el primer lugar en la columna “Orden de Vínculos”. 
4. Verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Controladores de dominio categoria alta - DL” aplica a todos los objetos del contenedor “Domain Controllers” y ocupa el primer lugar en el orden de vinculación.		En el árbol de la izquierda sitúese sobre el contenedor “Domain Controllers” desde: **“Bosque: [Su Bosque] → Dominios → [Su Dominio] → Domain Controllers”** En la pestaña “Objetos de Directiva de grupo vinculados” verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Controladores de dominio categoria alta - DL” figura en el panel de la derecha y ocupa el primer lugar en la columna “Orden de Vínculos”. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>5. Verifique la directiva de contraseñas en el objeto de directiva “CCN-STIC-570A ENS incremental Dominio categoria alta - DL”.</td><td></td><td>
En el “Administrador de Directivas de Grupo” pulse el botón derecho del ratón sobre la directiva desde:
“Bosque: [Su Bosque] → Dominios → [Su Dominio] → CCN-STIC-570A ENS incremental Dominio categoria alta - DL ”
Seleccione la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.


Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de contraseñas”


<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Almacenar contraseñas usando cifrado reversible</td><td>Deshabilitada</td><td></td></tr>
<tr><td>Exigir historial de contraseñas</td><td>24 contraseñas recordadas</td><td></td></tr>
<tr><td>Las contraseñas deben cumplir los requisitos de complejidad</td><td>Habilitada</td><td></td></tr>
<tr><td>Longitud mínima de la contraseña</td><td>10 caracteres</td><td></td></tr>
<tr><td>Vigencia máxima de la contraseña</td><td>45 días</td><td></td></tr>
<tr><td>Vigencia mínima de la contraseña</td><td>2 días</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>6. Verifique las directivas de bloqueo de cuenta de la directiva de grupo “CCN-STIC-570A ENS incremental Dominio categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de bloqueo de cuenta”</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Duración del bloqueo de cuenta</td><td>0</td><td></td></tr>
<tr><td>Restablecer recuentos de bloqueo de cuenta tras</td><td>30 minutos</td><td></td></tr>
<tr><td>Umbral de bloqueo de cuenta</td><td>8 intentos de inicio de sesión no válidos</td><td></td></tr>
</table></td></tr>
<tr><td>7. Verifique las directivas Kerberos en la directiva de grupo “CCN-STIC-570A ENS incremental Dominio categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva Kerberos”</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Aplicar restricciones de inicio de sesión de usuario</td><td>Habilitada</td><td></td></tr>
<tr><td>Tolerancia máxima para la sincronización de los relojes de los equipos</td><td>10 minutos</td><td></td></tr>
<tr><td>Vigencia máxima de renovación de vales de usuario</td><td>2 días</td><td></td></tr>
<tr><td>Vigencia máxima del vale de servicio</td><td>240 minutos</td><td></td></tr>
<tr><td>Vigencia máxima del vale de usuario</td><td>4 horas</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>8. Verifique las opciones de seguridad de la directiva de grupo “CCN-STIC-570A ENS incremental Dominio categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas Locales → Opciones de seguridad”
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Acceso de red: permitir traducción SID/nombre anónima</td><td>Deshabilitada</td><td></td></tr>
<tr><td>Seguridad de red: configurar tipos de cifrado permitidos para Kerberos</td><td>DES_CBC_CRC (Deshabilitado)
DES_CBC_MD5 (Deshabilitado)
RC4_HMAC_MD5 (Deshabilitado)
AES128_HMAC_SHA1 (Habilitado)
AES256_HMAC_SHA1 (Habilitado)
Tipos de cifrado futuros (Habilitado)</td><td></td></tr>
</table></td></tr>
<tr><td>9. Verifique las directivas de auditoría en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”.</td><td></td><td>En el “Administrador de Directivas de Grupo” pulse el botón derecho del ratón sobre la directiva desde:
“Bosque: [Su Bosque] → Dominios → [Su Dominio] → Domain Controllers → CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”
Seleccione la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 

Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Auditar el acceso a objetos</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar el acceso del servicio de directorio</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar el cambio de directivas</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar el seguimiento de procesos</td><td>Sin auditoría</td><td></td></tr>
<tr><td>Auditar el uso de privilegios</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar eventos de inicio de sesión</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar eventos de inicio de sesión de cuenta</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar eventos del sistema</td><td>Correcto</td><td></td></tr>
<tr><td>Auditar la administración de cuentas</td><td>Correcto, Erróneo</td><td></td></tr>
</table></td></tr>
<tr><td rowspan="2">10. Verifique la asignación de derechos de usuario en la directiva “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”</td></tr>
<tr><td colspan="4"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Administrar registro de seguridad y auditoría</td><td>Administradores</td><td></td></tr>
<tr><td>Agregar estaciones de trabajo al dominio</td><td>Administradores</td><td></td></tr>
<tr><td>Ajustar las cuotas de la memoria para un proceso</td><td>Administradores, SERVICIO LOCAL, Servicio de red</td><td></td></tr>
<tr><td>Apagar el sistema</td><td>Administradores</td><td></td></tr>
<tr><td>Aumentar el espacio de trabajo de un proceso</td><td>Administradores, SERVICIO LOCAL</td><td></td></tr>
<tr><td>Aumentar prioridad de programación</td><td>Administradores</td><td></td></tr>
<tr><td>Bloquear páginas en la memoria</td><td>Administradores</td><td></td></tr>
<tr><td>Cambiar la hora del sistema</td><td>SERVICIO LOCAL, Administradores</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Cambiar la zona horaria	SERVICIO LOCAL, Administradores	
		Cargar y descargar controladores de dispositivo	Administradores	
		Crear objetos globales	Administradores, SERVICIO, SERVICIO LOCAL, Servicio de red	
		Crear un archivo de paginación	Administradores	
		Crear vínculos simbólicos	Administradores	
		Denegar el acceso desde la red a este equipo	ANONYMOUS LOGON, Invitados	
		Denegar el inicio de sesión como servicio	Invitados	
		Denegar el inicio de sesión como trabajo por lotes	Invitados	
		Denegar el inicio de sesión local	Invitados	
		Denegar inicio de sesión a través de Servicios de Escritorio Remoto	Invitados	
		Forzar cierre desde un sistema remoto	Administradores	
		Generar auditorías de seguridad	SERVICIO LOCAL, Servicio de red	
		Generar perfiles de un solo proceso	Administradores	
		Generar perfiles del rendimiento del sistema	Administradores	
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	Administradores	
		Hacer copias de seguridad de archivos y directorios	Administradores, Operadores de copia de seguridad	
		Modificar la etiqueta de un objeto	Administradores	
		Modificar valores de entorno firmware	Administradores	
		Permitir el inicio de sesión local	Administradores	
		Quitar equipo de la estación de acoplamiento	Administradores	
		Realizar tareas de mantenimiento de volumen	Administradores	
		Reemplazar un símbolo (token) de nivel de proceso	SERVICIO LOCAL, Servicio de red	
		Restaurar archivos y directorios	Administradores	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="4"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Suplantar a un cliente tras la autenticación</td><td>Administradores, SERVICIO, SERVICIO LOCAL, Servicio de red</td><td></td></tr>
<tr><td colspan="2">Tener acceso a este equipo desde la red</td><td>Administradores, Usuarios autentificados, ENTERPRISE DOMAIN CONTROLLERS</td><td></td></tr>
<tr><td colspan="2">Tomar posesión de archivos y otros objetos</td><td>Administradores</td><td></td></tr>
<tr><td rowspan="6">11. Verifique las opciones de seguridad en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Acceso a redes: modelo de seguridad y uso compartido para cuentas locales</td><td>Clásico: usuarios locales se autentican con credenciales propias</td><td></td></tr>
<tr><td colspan="2">Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos</td><td>Deshabilitada</td><td></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos	Habilitada	
		Acceso a redes: rutas del Registro accesibles remotamente	System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, Software\Microsoft\Windows NT\CurrentVersion	
		Acceso a redes: rutas y subrutas del Registro accesibles remotamente	Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib, System\CurrentControlSet\Services\SysmonLog	
		Acceso a red: permitir traducción SID/nombre anónima	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Apagado: borrar el archivo de paginación de la memoria virtual	Habilitada	
		Apagado: permitir apagar el sistema sin tener que iniciar sesión	Deshabilitada	
		Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad	Habilitada	
		Auditoría: auditar el acceso de objetos globales del sistema	Habilitada	
		Auditoría: auditar el uso del privilegio de copias de seguridad y restauración	Habilitada	
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitada	
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitada	
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada	
		Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitada	
		Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitada	
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitada	
		Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador	Pedir credenciales en el escritorio seguro	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar	Pedir credenciales en el escritorio seguro	
		Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación	Habilitada	
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitada	
		Control de cuentas de usuario: elevar solo aplicaciones UIAccess instaladas en ubicaciones seguras	Habilitada	
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitada	
		Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitada	
		Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de Registro en diferentes ubicaciones por usuario	Habilitada	
		Controlador de dominio: no permitir los cambios de contraseña de cuenta de equipo	Deshabilitada	
		Controlador de dominio: permitir a los operadores de servidor programar tareas	Deshabilitada	
		Controlador de dominio: requisitos de firma de servidor LDAP	Requerir firma	
		Criptografía de sistema: forzar la protección con claves seguras para las claves de usuario almacenadas en el equipo	El usuario debe escribir una contraseña cada vez que use una clave.	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash	Habilitada	
		Cuentas: estado de la cuenta de invitado	Deshabilitada	
		Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitada	
		DCOM: restricciones de acceso al equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)	O:BAG:BAD:(A;;CCDCLC;;;AU)(A;;CCDCLC;;;S-1-5-32-562)	
		DCOM: restricciones de inicio al equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)	O:BAG:BAD:(A;;CCDCLCSWRP;;;BA)(A;;CCDCSW;;;AU)(A;;CCDCLCSWRP;;;S-1-5-32-562)	
		Dispositivos: impedir que los usuarios instalen controladores de impresora	Habilitada	
		Dispositivos: permitir desacoplamiento sin tener que iniciar sesión	Deshabilitada	
		Dispositivos: permitir formatear y expulsar medios extraíbles	Administradores	
		Dispositivos: restringir el acceso a disquetes sólo al usuario con sesión iniciada localmente	Habilitada	
		Dispositivos: restringir el acceso al CD-ROM sólo al usuario con sesión iniciada localmente	Habilitada	
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo	
		Inicio de sesión interactivo: mostrar información del usuario cuando se bloquee la sesión	No mostrar la información del usuario	
		Inicio de sesión interactivo: no mostrar el último nombre de usuario	Habilitada	
		Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr	Deshabilitada	
		Directiva	Valor	OK/NOK

Comprobación	OK/NOK	Cómo hacerlo	
	Inicio de sesión interactivo: número de inicios de sesión anteriores que se almacenarán en caché (si el controlador de dominio no está disponible)	0 inicios de sesión	
	Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire	14 días	
	Inicio de sesión interactivo: requerir la autenticación del controlador de dominio para desbloquear la estación de trabajo	Habilitada	
	Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	
	Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitada	
	Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitada	
	Miembro de dominio: duración máxima de contraseña de cuenta de equipo	30 días	
	Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	
	Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitada	
	Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitada	
	Seguridad de red: nivel de autenticación de LAN Manager	Enviar sólo respuesta NTLMv2 y rechazar LM	
	Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada	
	Seguridad de red: permitir que LocalSystem use la identidad del equipo para NTLM	Habilitada	
	Directiva	**Valor**	**OK/NOK**
	Seguridad de red: permitir	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo	
	retroceso a sesión NULL de LocalSystem		
	Seguridad de red: permitir solicitudes de autenticación PKU2U a este equipo para usar identidades en Internet.	Deshabilitada	
	Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma	
	Seguridad de red: restringir NTLM: auditar el tráfico NTLM entrante	Habilitar la auditoría para todas las cuentas	
	Seguridad de red: restringir NTLM: auditar la autenticación NTLM en este dominio	Habilitar todo	
	Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio	Denegar para cuentas de dominio en servidores de dominio	
	Seguridad de red: Restringir NTLM: tráfico NTLM entrante	Denegar todas las cuentas de dominio	
	Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)	Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits	
	Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)	Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits	
	Servidor de red Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitada	
	Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitada	
	Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada	
	Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor	Requerido del cliente	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td></td><td colspan="2">Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión</td><td>15 minutos</td><td></td></tr>
<tr><td rowspan="11">12. Verifique el registro de eventos en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro de Eventos”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Evitar que el grupo de invitados locales tenga acceso al registro de aplicaciones</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Evitar que el grupo de invitados locales tenga acceso al registro de seguridad</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Evitar que el grupo de invitados locales tenga acceso al registro del sistema</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Método de retención del registro de la aplicación</td><td>Según se necesite</td><td></td></tr>
<tr><td colspan="2">Método de retención del registro de seguridad</td><td>Según se necesite</td><td></td></tr>
<tr><td colspan="2">Método de retención del registro del sistema</td><td>Según se necesite</td><td></td></tr>
<tr><td colspan="2">Tamaño máximo del registro de la aplicación</td><td>32768 kilobytes</td><td></td></tr>
<tr><td colspan="2">Tamaño máximo del registro de seguridad</td><td>163840 kilobytes</td><td></td></tr>
<tr><td colspan="2">Tamaño máximo del registro del sistema</td><td>32768 kilobytes</td><td></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
13. Verifique los servicios del sistema en la directiva de grupo "CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL".		Seleccione el siguiente nodo. **"Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"** **Nota:** Dependiendo de los servicios que estén instalados en el equipo, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales (antivirus, etc.). En la siguiente tabla se muestran el nombre largo y el nombre corto para cada servicio. En la ventana del editor de administración de directivas de grupo sólo aparecerá uno de los dos: el nombre largo si el servicio está instalado en el sistema o el nombre corto si no lo está. Además, deberá tener en cuenta que los números existentes en algunos servicios son aleatorios y cambian en cada equipo.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado	
Administración de aplicaciones	AppMgmt	Manual	Configurado	
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado	
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado	
Administración remota de Windows (WS-Management)	WinRM	Automático	Configurado	
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado	
Administrador de conexiones de acceso remoto	RasMan	Manual	Configurado	
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado	
Administrador de credenciales	VaultSvc	Manual	Configurado	
Administrador de cuentas de seguridad	SamSs	Automático	Configurado	
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado	
Administrador de sesión local	LSM	Automático	Configurado	
Administrador de usuarios	UserManager	Automático	Configurado	
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado	
Agente de conexión de red	NcbService	Manual	Configurado	
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado	
Agente de directiva IPsec	PolicyAgent	Manual	Configurado	
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado	
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado	
Aislamiento de claves CNG	KeyIso	Manual	Configurado	
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado	
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado	
Aplicación auxiliar IP	iphlpsvc	Automático	Configurado	
Aplicación del sistema COM+	COMSysApp	Manual	Configurado	
Archivos sin conexión	CscService	Deshabilitado	Configurado	
Asignador de detección de topologías de nivel de vínculo	lltdsvc	Manual	Configurado	
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**

Comprobación	OK/NOK	Cómo hacerlo		
Asistente para la conectividad de red	NcaSvc	Manual	Configurado	
Audio de Windows	Audiosrv	Manual	Configurado	
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Deshabilitado	Configurado	
Ayudante especial de la consola de administración	sacsvr	Manual	Configurado	
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado	
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado	
CDPUserSvc	CDPUserSvc	Automático	Configurado	
Centro de distribución de claves Kerberos	Kdc	Automático	Configurado	
Cliente de directiva de grupo	gpsvc	Automático	Configurado	
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático	Configurado	
Cliente DHCP	Dhcp	Automático	Configurado	
Cliente DNS	Dnscache	Automático	Configurado	
Cola de impresión	Spooler	Automático	Configurado	
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Manual	Configurado	
Comprobador puntual	svsvc	Manual	Configurado	
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado	
Conexiones de red	Netman	Manual	Configurado	
Configuración automática de redes cableadas	dot3svc	Manual	Configurado	
Configuración de Escritorio remoto	SessionEnv	Manual	Configurado	
Conjunto resultante de proveedor de directivas	RSoPProv	Manual	Configurado	
Contenedor de Microsoft Passport	NgcCtnrSvc	Manual	Configurado	
Coordinador de transacciones distribuidas	MSDTC	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
CoreMessaging	CoreMessagingRegistra	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
		r			
DataCollectionPublishingService		DcpSvc	Manual	Configurado	
Datos de contactos		PimIndexMaintenanceSvc	Manual	Configurado	
Detección de hardware shell		ShellHWDetection	Deshabilitado	Configurado	
Detección de servicios interactivos		UI0Detect	Manual	Configurado	
Detección SSDP		SSDPSRV	Deshabilitado	Configurado	
Directiva de extracción de tarjetas inteligentes		SCPolicySvc	Manual	Configurado	
Disco virtual		vds	Manual	Configurado	
Dispositivo host de UPnP		upnphost	Manual	Configurado	
DLL de host del Contador de rendimiento		PerfHost	Manual	Configurado	
dmwappushsvc		dmwappushservice	Deshabilitado	Configurado	
Energía		Power	Automático	Configurado	
Enrutamiento y acceso remoto		RemoteAccess	Deshabilitado	Configurado	
Espacio de nombres DFS		Dfs	Automático	Configurado	
Estación de trabajo		LanmanWorkstation	Automático	Configurado	
Eventos de adquisición de imágenes estáticas		WiaRpc	Manual	Configurado	
Examinador de equipos		Browser	Deshabilitado	Configurado	
Experiencia de calidad de audio y vídeo de Windows (qWave)		QWAVE	Deshabilitado	Configurado	
Extensiones y notificaciones de impresora		PrintNotify	Manual	Configurado	
Firewall de Windows		MpsSvc	Automático	Configurado	
Hora de Windows		W32Time	Automático	Configurado	
Host de proveedor de detección de función		fdPHost	Deshabilitado	Configurado	
Host de sistema de diagnóstico		WdiSystemHost	Deshabilitado	Configurado	
Host del servicio de diagnóstico		WdiServiceHost	Deshabilitado	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Identidad de aplicación		AppIDSvc	Manual	Configurado	
Información de la		Appinfo	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
aplicación					
Iniciador de procesos de servidor DCOM		DcomLaunch	Automático	Configurado	
Inicio de sesión secundario		seclogon	Deshabilitado	Configurado	
Instalador de ActiveX (AxInstSV)		AxInstSV	Manual	Configurado	
Instalador de módulos de Windows		TrustedInstaller	Manual	Configurado	
Instantáneas de volumen		VSS	Manual	Configurado	
Instrumental de administración de Windows		Winmgmt	Automático	Configurado	
Interfaz de servicio invitado de Hyper-V		vmicguestinterface	Manual	Configurado	
KTMRM para DTC (Coordinador de transacciones distribuidas)		KtmRm	Manual	Configurado	
Llamada a procedimiento remoto (RPC)		RpcSs	Automático	Configurado	
Mensajería entre sitios		IsmServ	Automático	Configurado	
Microsoft App-V Client		AppVClient	Deshabilitado	Configurado	
Microsoft Passport		NgcSvc	Manual	Configurado	
Modo incrustado		embeddedmode	Manual	Configurado	
Módulos de creación de claves de IPsec para IKE y AuthIP		IKEEXT	Manual	Configurado	
Motor de filtrado de base		BFE	Automático	Configurado	
Net Logon		Netlogon	Automático	Configurado	
Optimizar unidades		defragsvc	Manual	Configurado	
Partida guardada en Xbox Live		XblGameSave	Deshabilitado	Configurado	
Plug and Play		PlugPlay	Manual	Configurado	
Preparación de aplicaciones		AppReadiness	Manual	Configurado	
Programador de tareas		Schedule	Automático	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Propagación de certificados		CertPropSvc	Manual	Configurado	
Protección de software		sppsvc	Automático	Configurado	
Protocolo de		Eaphost	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
autenticación extensible					
Proveedor de instantáneas de software de Microsoft		swprv	Manual	Configurado	
Publicación de recurso de detección de función		FDResPub	Deshabilitado	Configurado	
Reconoc. ubicación de red		NlaSvc	Automático	Configurado	
Recopilador de eventos de Windows		Wecsvc	Manual	Configurado	
Redirector de puerto en modo usuario de Servicios de Escritorio remoto		UmRdpService	Manual	Configurado	
Registro de eventos de Windows		EventLog	Automático	Configurado	
Registro remoto		RemoteRegistry	Automático	Configurado	
Registros y alertas de rendimiento		pla	Manual	Configurado	
Replicación de archivos		NtFrs	Deshabilitado	Configurado	
Replicación DFS		DFSR	Automático	Configurado	
Servicio Asistente para la compatibilidad de programas		PcaSvc	Automático	Configurado	
Servicio biométrico de Windows		WbioSrvc	Manual	Configurado	
Servicio de actualizaciones Orchestrator para Windows Update		UsoSvc	Manual	Configurado	
Servicio de administración de aplicaciones de empresa		EntAppSvc	Manual	Configurado	
Servicio de administración de radio		RmSvc	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de administrador de licencias de Windows		LicenseManager	Manual	Configurado	
Servicio de almacenamiento		StorSvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio de asociación de dispositivos		DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows		FontCache	Deshabilitado	Configurado	
Servicio de cierre de invitado de Hyper-V		vmicshutdown	Manual	Configurado	
Servicio de compatibilidad con Bluetooth		bthserv	Manual	Configurado	
Servicio de configuración de red		NetSetupSvc	Manual	Configurado	
Servicio de datos del sensor		SensorDataService	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP		WinHttpAutoProxySvc	Manual	Configurado	
Servicio de directivas de diagnóstico		DPS	Deshabilitado	Configurado	
Servicio de dispositivo de interfaz humana		hidserv	Manual	Configurado	
Servicio de distribución de clave de Microsoft		KdsSvc	Manual	Configurado	
Servicio de enrutador de AllJoyn		AJRouter	Deshabilitado	Configurado	
Servicio de enumeración de dispositivos de tarjeta inteligente		ScDeviceEnum	Manual	Configurado	
Servicio de geolocalización		lfsvc	Manual	Configurado	
Servicio de host HV		HvHost	Manual	Configurado	
Servicio de implementación de AppX (AppXSVC)		AppXSvc	Manual	Configurado	
Servicio de infraestructura de tareas en segundo plano		BrokerInfrastructure	Automático	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de inscripción de administración de dispositivos		DmEnrollmentSvc	Manual	Configurado	
Servicio de inspección de red de Windows Defender		WdNisSvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio de instalación de dispositivos	DeviceInstall	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado	
Servicio de licencia de cliente (ClipSVC)	ClipSVC	Manual	Configurado	
Servicio de lista de redes	netprofm	Manual	Configurado	
Servicio de notificación de eventos de sistema	SENS	Automático	Configurado	
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService	Deshabilitado	Configurado	
Servicio de perfil de usuario	ProfSvc	Automático	Configurado	
Servicio de plataforma de dispositivos conectados	CDPSvc	Automático	Configurado	
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Manual	Configurado	
Servicio de puerta de enlace de nivel de aplicación	ALG	Manual	Configurado	
Servicio de registro de acceso de usuarios	UALSVC	Automático	Configurado	
Servicio de repositorio de estado	StateRepository	Manual	Configurado	
Servicio de sensores	SensorService	Manual	Configurado	
Servicio de servidor proxy KDC (KPS)	KPSSVC	Manual	Configurado	
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de supervisión de licencias de Windows	WLMS	Automático	Configurado	
Servicio de supervisión de sensores	SensrSvc	Manual	Configurado	
Servicio de transferencia inteligente en segundo	BITS	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
plano (BITS)					
Servicio de uso compartido de datos		DsSvc	Manual	Configurado	
Servicio de uso compartido de puertos Net.Tcp		NetTcpPortSharing	Deshabilitado	Configurado	
Servicio de usuario de notificaciones de inserción de Windows		WpnUserService	Manual	Configurado	
Servicio de virtualización de Escritorio remoto de Hyper-V		vmicrdv	Manual	Configurado	
Servicio de virtualización de la experiencia de usuario		UevAgentService	Deshabilitado	Configurado	
Servicio de Windows Defender		WinDefend	Automático	Configurado	
Servicio de Windows Insider		wisvc	Manual	Configurado	
Servicio de zona con cobertura inalámbrica móvil de Windows		icssvc	Deshabilitado	Configurado	
Servicio del iniciador iSCSI de Microsoft		MSiSCSI	Manual	Configurado	
Servicio del sistema de notificaciones de inserción de Windows		WpnService	Automático	Configurado	
Servicio enumerador de dispositivos portátiles		WPDBusEnum	Manual	Configurado	
Servicio FrameServer de la Cámara de Windows		FrameServer	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio host de proveedor de cifrado de Windows		WEPHOSTSVC	Manual	Configurado	
Servicio Informe de errores de Windows		WerSvc	Deshabilitado	Configurado	
Servicio Interfaz de almacenamiento en red		nsi	Automático	Configurado	
Servicio PowerShell Direct de Hyper-V		vmicvmsession	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)		diagnosticshub.standardcollector.service	Manual	Configurado	
Servicio telefónico		PhoneSvc	Manual	Configurado	
Servicios de cifrado		CryptSvc	Automático	Configurado	
Servicios de dominio de Active Directory		NTDS	Automático	Configurado	
Servicios de Escritorio remoto		TermService	Manual	Configurado	
Servicios web de Active Directory		ADWS	Automático	Configurado	
Servidor		LanmanServer	Automático	Configurado	
Servidor de roles de DS		DsRoleSvc	Manual	Configurado	
Servidor del modelo de datos del mosaico		tiledatamodelsvc	Automático	Configurado	
Servidor DNS		DNS	Automático	Configurado	
Sincronizar host		OneSyncSvc	Automático	Configurado	
Sistema de cifrado de archivos (EFS)		EFS	Manual	Configurado	
Sistema de eventos COM+		EventSystem	Automático	Configurado	
SMP de Espacios de almacenamiento de Microsoft		smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V		vmicvss	Manual	Configurado	
Superfetch		SysMain	Manual	Configurado	
Tarjeta inteligente		SCardSvr	Deshabilitado	Configurado	
Telefonía		TapiSrv	Deshabilitado	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Telemetría y experiencias del usuario conectado		DiagTrack	Automático	Configurado	
Temas		Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)		RpcLocator	Manual	Configurado	
WalletService		WalletService	Manual	Configurado	
Windows Driver Foundation - User-mode Driver Framework		wudfsvc	Manual	Configurado	

<table>
<tr><th>Comprobación</th><th colspan="2">OK/NOK</th><th colspan="4">Cómo hacerlo</th></tr>
<tr><td colspan="2">Windows Installer</td><td>msiserver</td><td>Manual</td><td>Configurado</td><td></td></tr>
<tr><td colspan="2">Windows Search</td><td>WSearch</td><td>Deshabilitado</td><td>Configurado</td><td></td></tr>
<tr><td colspan="2">Windows Update</td><td>wuauserv</td><td>Manual</td><td>Configurado</td><td></td></tr>
<tr><td>14. Verifique los permisos de valores de registro de la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”.</td><td></td><td colspan="4">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro”

Nota: Para verificar los permisos de la entrada de registro, deberá pulsar doble clic sobre la entrada “MACHINES → SOFTWARE → Microsoft → Windows → CurrentVersion → Installer” y pulsar sobre el botón "Modificar seguridad...".

Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".</td></tr>
<tr><td></td><td colspan="2">Directiva</td><td colspan="2">Valor</td><td>OK/NOK</td></tr>
<tr><td></td><td colspan="2">MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer</td><td colspan="2">Administradores: Control Total
SYSTEM: Control Total
Usuarios: Leer</td><td></td></tr>
<tr><td>15. Verifique los valores del sistema de archivos de la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”.</td><td></td><td colspan="4">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de Archivos”

Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción “Propiedades” del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...".

Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\Registration	Administrador	Control total	
	System	Control total	
	Usuario	Leer y ejecutar	
%SystemRoot%\repair	Administrador	Control total	
	System	Control total	
%SystemRoot%\security	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\cacls.exe	Administrador	Control total	
	System	Control total	

Archivo	Usuario	Permiso	OK/NOK
SystemRoot%\system32\clip.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\ras	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\rasadhlp.dll	Administrador	Control total	
%SystemRoot%\system32\rasauto.dll	Administrador	Control total	
%SystemRoot%\system32\rasautou.exe	Administrador	Control total	
%SystemRoot%\system32\raschap.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrnm.h	Administrador	Control total	
%SystemRoot%\system32\rasctrs.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrs.ini	Administrador	Control total	
%SystemRoot%\system32\rasdial.exe	Administrador	Control total	
%SystemRoot%\system32\rasmans.dll	Administrador	Control total	
%SystemRoot%\system32\rasmontr.dll	Administrador	Control total	
%SystemRoot%\system32\rasphone.exe	Administrador	Control total	
%SystemRoot%\system32\rasppp.dll	Administrador	Control total	
%SystemRoot%\system32\rastapi.dll	Administrador	Control total	
%SystemRoot%\system32\rastls.dll	Administrador	Control total	
%SystemRoot%\system32\runonce.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\secedit.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\telnet.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tftp.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tracert.exe	Administrador	Control total	
	System	Control total	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>16. Verifique que está bloqueada la ejecución del Almacén digital en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Administración de derechos digitales de Windows Media”</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Impedir el acceso a internet de Windows Media DRM</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td>17. Verifique que está bloqueada la ejecución del Almacén digital en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Almacén Digital”</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>No permitir que se ejecute el Almacén digital</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
</table>

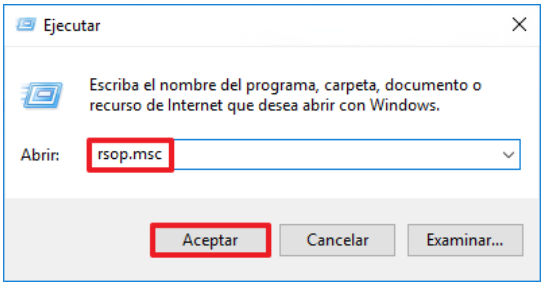
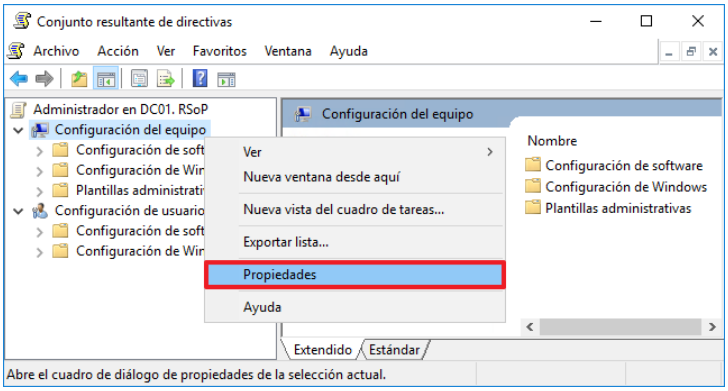
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>18. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Biometría”</td></tr>
<tr><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Permitir el uso de biometría</td><td>Habilitada</td><td></td></tr>
<tr><td>Permitir que los usuarios de dominio inicien sesión mediante biometría</td><td>Habilitada</td><td></td></tr>
<tr><td>Permitir que los usuarios inicien sesión mediante biometría</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td>19. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Directivas de reproducción automática”</td></tr>
<tr><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Desactivar reproducción automática</td><td>Habilitada</td><td></td></tr>
<tr><td>Establecer el comportamiento predeterminado para ejecución automática.</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
</table>

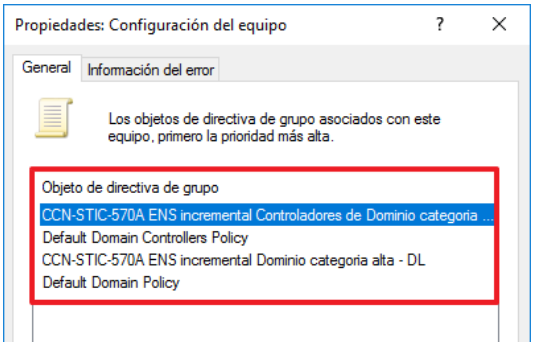
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td rowspan="4">20. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”.</td><td></td><td colspan="2">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Informe de errores de Windows”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Deshabilitar el informe de errores de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">No enviar datos adicionales</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="4">21. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”.</td><td></td><td colspan="2">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Opciones de inicio de sesión de Windows”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Informar cuando el servidor de inicio de sesión no está disponible durante el inicio de sesión del usuario</td><td>Habilitada</td><td></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>22. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Shell remoto de Windows”

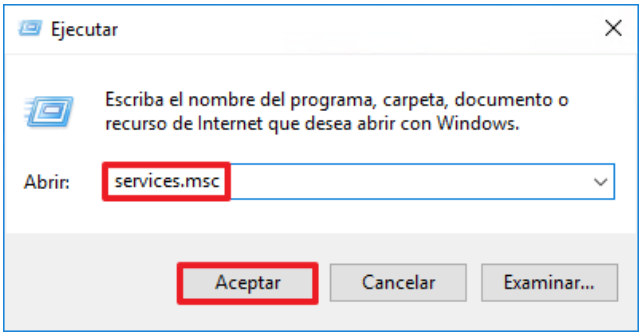
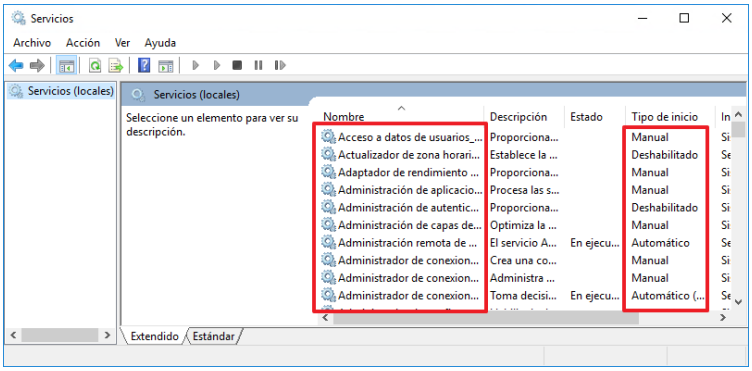
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Permitir acceso a Shell remoto</td><td>Deshabilitada</td><td></td></tr>
</table>
</td></tr>
<tr><td>23. Verifique configuración de la comunicación de Internet en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Desactivar informe de errores de reconocimiento de escritura a mano</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el Programa para la mejora de la experiencia del usuario de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar los vínculos “Events.asp” del Visor de eventos</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el contenido “¿Sabía que…?” del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la búsqueda en Microsoft Knowledge Base del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el informe de errores de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la actualización de archivos de contenido del Asistente para búsqueda</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el acceso a la Tienda</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la tarea de imágenes “Pedir copias fotográficas”</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td>24. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL”.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Sistema → Net Logon”</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Permitir algoritmos de criptografía compatibles con Windows NT 4.0</td><td>Deshabilitada</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
25. Verifique que el equipo ha recibido las directivas de grupo CC-STIC-570A ENS incremental Dominio categoria alta - DL y CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL		Ejecute la consola de administración "Conjunto resultante de directivas" (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → rsop.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" para continuar. 
		Seleccione en ella la rama "Configuración del equipo", márquela con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la figura: 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", resaltada en la siguiente figura:
 

Verifique que en dicha sección aparecen listados, y por ese orden, los objetos de directiva de grupo que se indican en la siguiente tabla:
<table>
<tr><th>Objeto de directiva de grupo</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-570A ENS incremental Controladores de Dominio categoria alta - DL</td><td></td></tr>
<tr><td>Default Domain Controllers Policy</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS incremental Dominio categoria alta - DL</td><td></td></tr>
<tr><td>Default Domain Policy</td><td></td></tr>
</table>
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
26. Verifique que los servicios del sistema están correctamente configurados		Usando la consola de servicios (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → services.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" para continuar.  Verifique que el tipo de inicio de los servicios que aparecen en el sistema y en la siguiente tabla coinciden:  **Nota:** Dependiendo del equipo, es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales (antivirus, etc.).

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado	
Administración de aplicaciones	AppMgmt	Manual	Configurado	
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado	
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado	
Administración remota de Windows (WS-Management)	WinRM	Automático	Configurado	
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado	
Administrador de conexiones de acceso remoto	RasMan	Manual	Configurado	
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado	
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado	
Administrador de credenciales	VaultSvc	Manual	Configurado	
Administrador de cuentas de seguridad	SamSs	Automático	Configurado	
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado	
Administrador de sesión local	LSM	Automático	Configurado	
Administrador de usuarios	UserManager	Automático	Configurado	
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**

Comprobación	OK/NOK	Cómo hacerlo		
Agente de conexión de red	NcbService	Manual	Configurado	
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado	
Agente de directiva IPsec	PolicyAgent	Manual	Configurado	
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado	
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado	
Aislamiento de claves CNG	KeyIso	Manual	Configurado	
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado	
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado	
Aplicación auxiliar IP	iphlpsvc	Automático	Configurado	
Aplicación del sistema COM+	COMSysApp	Manual	Configurado	
Archivos sin conexión	CscService	Deshabilitado	Configurado	
Asignador de detección de topologías de nivel de vínculo	lltdsvc	Manual	Configurado	
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado	
Asistente para la conectividad de red	NcaSvc	Manual	Configurado	
Audio de Windows	Audiosrv	Manual	Configurado	
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Deshabilitado	Configurado	
Ayudante especial de la consola de administración	sacsvr	Manual	Configurado	
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado	
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado	
CDPUserSvc	CDPUserSvc	Automático	Configurado	
Centro de distribución de claves Kerberos	Kdc	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Cliente de directiva de grupo	gpsvc	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Cliente de seguimiento de vínculos distribuidos		TrkWks	Automático	Configurado	
Cliente DHCP		Dhcp	Automático	Configurado	
Cliente DNS		Dnscache	Automático	Configurado	
Cola de impresión		Spooler	Automático	Configurado	
Compilador de extremo de audio de Windows		AudioEndpointBuilder	Manual	Configurado	
Comprobador puntual		svsvc	Manual	Configurado	
Conexión compartida a Internet (ICS)		SharedAccess	Deshabilitado	Configurado	
Conexiones de red		Netman	Manual	Configurado	
Configuración automática de redes cableadas		dot3svc	Manual	Configurado	
Configuración de Escritorio remoto		SessionEnv	Manual	Configurado	
Conjunto resultante de proveedor de directivas		RSoPProv	Manual	Configurado	
Contenedor de Microsoft Passport		NgcCtnrSvc	Manual	Configurado	
Coordinador de transacciones distribuidas		MSDTC	Automático	Configurado	
CoreMessaging		CoreMessagingRegistrar	Automático	Configurado	
DataCollectionPublishingService		DcpSvc	Manual	Configurado	
Datos de contactos		PimIndexMaintenanceSvc	Manual	Configurado	
Detección de hardware shell		ShellHWDetection	Deshabilitado	Configurado	
Detección de servicios interactivos		UI0Detect	Manual	Configurado	
Detección SSDP		SSDPSRV	Deshabilitado	Configurado	
Directiva de extracción de tarjetas inteligentes		SCPolicySvc	Manual	Configurado	
Disco virtual		vds	Manual	Configurado	
Dispositivo host de UPnP		upnphost	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
DLL de host del Contador de rendimiento		PerfHost	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
dmwappushsvc		dmwappushservice	Deshabilitado	Configurado	
Energía		Power	Automático	Configurado	
Enrutamiento y acceso remoto		RemoteAccess	Deshabilitado	Configurado	
Espacio de nombres DFS		Dfs	Automático	Configurado	
Estación de trabajo		LanmanWorkstation	Automático	Configurado	
Eventos de adquisición de imágenes estáticas		WiaRpc	Manual	Configurado	
Examinador de equipos		Browser	Deshabilitado	Configurado	
Experiencia de calidad de audio y vídeo de Windows (qWave)		QWAVE	Deshabilitado	Configurado	
Extensiones y notificaciones de impresora		PrintNotify	Manual	Configurado	
Firewall de Windows		MpsSvc	Automático	Configurado	
Hora de Windows		W32Time	Automático	Configurado	
Host de proveedor de detección de función		fdPHost	Deshabilitado	Configurado	
Host de sistema de diagnóstico		WdiSystemHost	Deshabilitado	Configurado	
Host del servicio de diagnóstico		WdiServiceHost	Deshabilitado	Configurado	
Identidad de aplicación		AppIDSvc	Manual	Configurado	
Información de la aplicación		Appinfo	Manual	Configurado	
Iniciador de procesos de servidor DCOM		DcomLaunch	Automático	Configurado	
Inicio de sesión secundario		seclogon	Deshabilitado	Configurado	
Instalador de ActiveX (AxInstSV)		AxInstSV	Manual	Configurado	
Instalador de módulos de Windows		TrustedInstaller	Manual	Configurado	
Instantáneas de volumen		VSS	Manual	Configurado	
Instrumental de administración de Windows		Winmgmt	Automático	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Interfaz de servicio invitado de Hyper-V		vmicguestinterface	Manual	Configurado	
KTMRM para DTC (Coordinador de		KtmRm	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
transacciones distribuidas)					
Llamada a procedimiento remoto (RPC)		RpcSs	Automático	Configurado	
Mensajería entre sitios		IsmServ	Automático	Configurado	
Microsoft App-V Client		AppVClient	Deshabilitado	Configurado	
Microsoft Passport		NgcSvc	Manual	Configurado	
Modo incrustado		embeddedmode	Manual	Configurado	
Módulos de creación de claves de IPsec para IKE y AuthIP		IKEEXT	Manual	Configurado	
Motor de filtrado de base		BFE	Automático	Configurado	
Net Logon		Netlogon	Automático	Configurado	
Optimizar unidades		defragsvc	Manual	Configurado	
Partida guardada en Xbox Live		XblGameSave	Deshabilitado	Configurado	
Plug and Play		PlugPlay	Manual	Configurado	
Preparación de aplicaciones		AppReadiness	Manual	Configurado	
Programador de tareas		Schedule	Automático	Configurado	
Propagación de certificados		CertPropSvc	Manual	Configurado	
Protección de software		sppsvc	Automático	Configurado	
Protocolo de autenticación extensible		Eaphost	Manual	Configurado	
Proveedor de instantáneas de software de Microsoft		swprv	Manual	Configurado	
Publicación de recurso de detección de función		FDResPub	Deshabilitado	Configurado	
Reconoc. ubicación de red		NlaSvc	Automático	Configurado	
Recopilador de eventos de Windows		Wecsvc	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Redirector de puerto en modo usuario de Servicios de Escritorio remoto		UmRdpService	Manual	Configurado	
Registro de eventos de Windows		EventLog	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Registro remoto		RemoteRegistry	Automático	Configurado	
Registros y alertas de rendimiento		pla	Manual	Configurado	
Replicación de archivos		NtFrs	Deshabilitado	Configurado	
Replicación DFS		DFSR	Automático	Configurado	
Servicio Asistente para la compatibilidad de programas		PcaSvc	Automático	Configurado	
Servicio biométrico de Windows		WbioSrvc	Manual	Configurado	
Servicio de actualizaciones Orchestrator para Windows Update		UsoSvc	Manual	Configurado	
Servicio de administración de aplicaciones de empresa		EntAppSvc	Manual	Configurado	
Servicio de administración de radio		RmSvc	Manual	Configurado	
Servicio de administrador de licencias de Windows		LicenseManager	Manual	Configurado	
Servicio de almacenamiento		StorSvc	Manual	Configurado	
Servicio de asociación de dispositivos		DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows		FontCache	Deshabilitado	Configurado	
Servicio de cierre de invitado de Hyper-V		vmicshutdown	Manual	Configurado	
Servicio de compatibilidad con Bluetooth		bthserv	Manual	Configurado	
Servicio de configuración de red		NetSetupSvc	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de datos del sensor		SensorDataService	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP		WinHttpAutoProxySvc	Manual	Configurado	
Servicio de directivas de diagnóstico		DPS	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio de dispositivo de interfaz humana	hidserv	Manual	Configurado	
Servicio de distribución de clave de Microsoft	KdsSvc	Manual	Configurado	
Servicio de enrutador de AllJoyn	AJRouter	Deshabilitado	Configurado	
Servicio de enumeración de dispositivos de tarjeta inteligente	ScDeviceEnum	Manual	Configurado	
Servicio de geolocalización	lfsvc	Manual	Configurado	
Servicio de host HV	HvHost	Manual	Configurado	
Servicio de implementación de AppX (AppXSVC)	AppXSvc	Manual	Configurado	
Servicio de infraestructura de tareas en segundo plano	BrokerInfrastructure	Automático	Configurado	
Servicio de inscripción de administración de dispositivos	DmEnrollmentSvc	Manual	Configurado	
Servicio de inspección de red de Windows Defender	WdNisSvc	Manual	Configurado	
Servicio de instalación de dispositivos	DeviceInstall	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado	
Servicio de licencia de cliente (ClipSVC)	ClipSVC	Manual	Configurado	
Servicio de lista de redes	netprofm	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de notificación de eventos de sistema	SENS	Automático	Configurado	
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService	Deshabilitado	Configurado	
Servicio de perfil de usuario	ProfSvc	Automático	Configurado	
Servicio de plataforma	CDPSvc	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
de dispositivos conectados				
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Manual	Configurado	
Servicio de puerta de enlace de nivel de aplicación	ALG	Manual	Configurado	
Servicio de registro de acceso de usuarios	UALSVC	Automático	Configurado	
Servicio de repositorio de estado	StateRepository	Manual	Configurado	
Servicio de sensores	SensorService	Manual	Configurado	
Servicio de servidor proxy KDC (KPS)	KPSSVC	Manual	Configurado	
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado	
Servicio de supervisión de licencias de Windows	WLMS	Automático	Configurado	
Servicio de supervisión de sensores	SensrSvc	Manual	Configurado	
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Manual	Configurado	
Servicio de uso compartido de datos	DsSvc	Manual	Configurado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Deshabilitado	Configurado	
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual	Configurado	
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado	
Servicio de Windows Defender	WinDefend	Automático	Configurado	

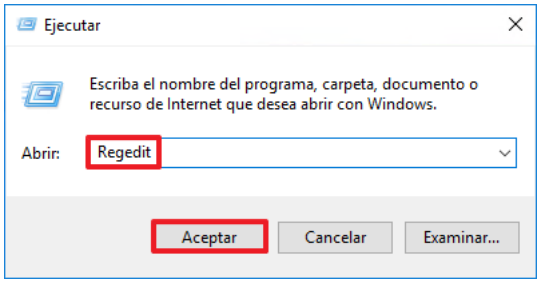
Comprobación	OK/NOK	Cómo hacerlo		
Servicio de Windows Insider	wisvc	Manual	Configurado	
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado	
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Manual	Configurado	
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado	
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Manual	Configurado	
Servicio FrameServer de la Cámara de Windows	FrameServer	Manual	Configurado	
Servicio host de proveedor de cifrado de Windows	WEPHOSTSVC	Manual	Configurado	
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado	
Servicio Interfaz de almacenamiento en red	nsi	Automático	Configurado	
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado	
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standardcollector.service	Manual	Configurado	
Servicio telefónico	PhoneSvc	Manual	Configurado	
Servicios de cifrado	CryptSvc	Automático	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicios de dominio de Active Directory	NTDS	Automático	Configurado	
Servicios de Escritorio remoto	TermService	Manual	Configurado	
Servicios web de Active Directory	ADWS	Automático	Configurado	
Servidor	LanmanServer	Automático	Configurado	
Servidor de roles de DS	DsRoleSvc	Manual	Configurado	
Servidor del modelo de datos del mosaico	tiledatamodelsvc	Automático	Configurado	
Servidor DNS	DNS	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Sincronizar host		OneSyncSvc	Automático	Configurado	
Sistema de cifrado de archivos (EFS)		EFS	Manual	Configurado	
Sistema de eventos COM+		EventSystem	Automático	Configurado	
SMP de Espacios de almacenamiento de Microsoft		smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V		vmicvss	Manual	Configurado	
Superfetch		SysMain	Manual	Configurado	
Tarjeta inteligente		SCardSvr	Deshabilitado	Configurado	
Telefonía		TapiSrv	Deshabilitado	Configurado	
Telemetría y experiencias del usuario conectado		DiagTrack	Automático	Configurado	
Temas		Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)		RpcLocator	Manual	Configurado	
WalletService		WalletService	Manual	Configurado	
Windows Driver Foundation - User-mode Driver Framework		wudfsvc	Manual	Configurado	
Windows Installer		msiserver	Manual	Configurado	
Windows Search		WSearch	Deshabilitado	Configurado	
Windows Update		wuauserv	Manual	Configurado	
27. Verifique que se han asignado los permisos correctos en el sistema de archivos		Utilizando el Explorador de Windows: **"Windows+R → Explorer"** En caso de no saber dónde apunta cada una de las rutas abreviadas que se especifica, ejecute Explorer <<ruta>> donde <<ruta>> se sustituirá por la ruta abreviada. **Nota:** Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, marcándolo con el botón derecho y eligiendo la opción "Propiedades" del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá situarse en la pestaña "Seguridad". En la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios. Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados.			

Comprobación	OK/NOK	Cómo hacerlo

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\Registration	Administrador	Control total	
	System	Control total	
	Usuario	Leer y ejecutar	
%SystemRoot%\repair	Administrador	Control total	
	System	Control total	
%SystemRoot%\security	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\cacls.exe	Administrador	Control total	
	System	Control total	
SystemRoot%\system32\clip.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\ras	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\rasadhlp.dll	Administrador	Control total	
%SystemRoot%\system32\rasauto.dll	Administrador	Control total	
%SystemRoot%\system32\rasautou.exe	Administrador	Control total	
%SystemRoot%\system32\raschap.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrnm.h	Administrador	Control total	
%SystemRoot%\system32\rasctrs.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrs.ini	Administrador	Control total	
%SystemRoot%\system32\rasdial.exe	Administrador	Control total	
%SystemRoot%\system32\rasmans.dll	Administrador	Control total	
%SystemRoot%\system32\rasmontr.dll	Administrador	Control total	
%SystemRoot%\system32\rasphone.exe	Administrador	Control total	
%SystemRoot%\system32\rasppp.dll	Administrador	Control total	
%SystemRoot%\system32\rastapi.dll	Administrador	Control total	
%SystemRoot%\system32\rastls.dll	Administrador	Control total	

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\system32\runonce.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\secedit.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\telnet.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tftp.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tracert.exe	Administrador	Control total	
	System	Control total	

Comprobación	OK/NOK	Cómo hacerlo
28. Verifique los valores del Registro.		Compruebe los valores del registro definidos en los Controladores de Dominio que pertenezcan al grupo categorizado como categoría alta siguiendo los criterios del ENS, mediante el uso del "Editor del Registro". **"Windows+R → Regedit"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" para continuar. 

Valor del registro	Valor	OK/NOK
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod	0	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun	255	
HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation	1	
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode	1	
HKLM\System\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta	10	
HKLM\System\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog	1	
HKLM\System\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog	20000	

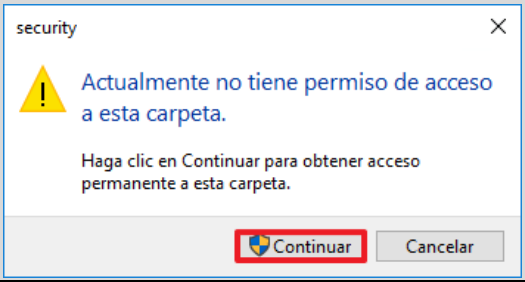
Comprobación	OK/NOK	Cómo hacerlo		
		Valor del registro	Valor	OK/NOK
		HKLM\System\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog	20	
		HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel	90	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect	0	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime	300000	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery	0	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect	1	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions	2	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions	3	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TCPMaxPortsExhausted	5	

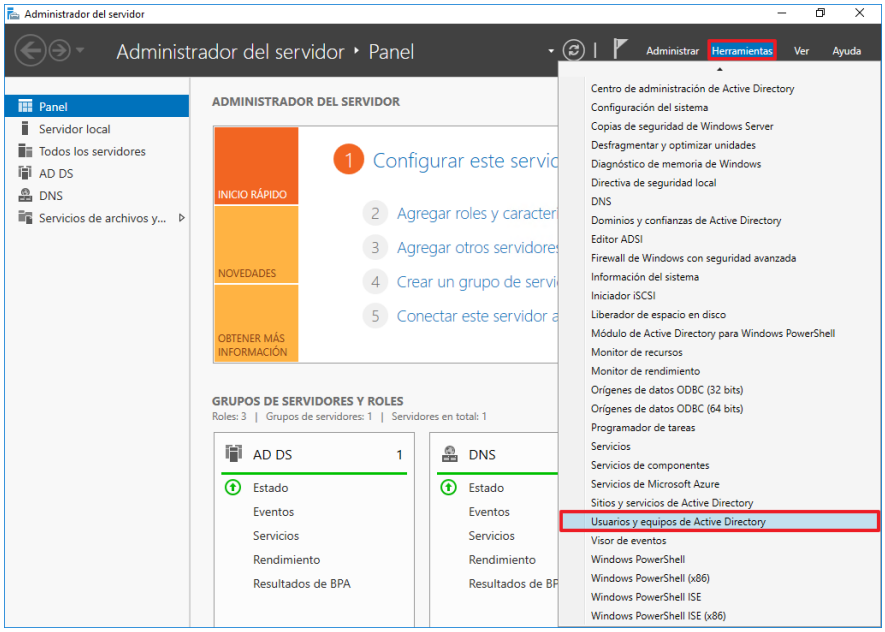
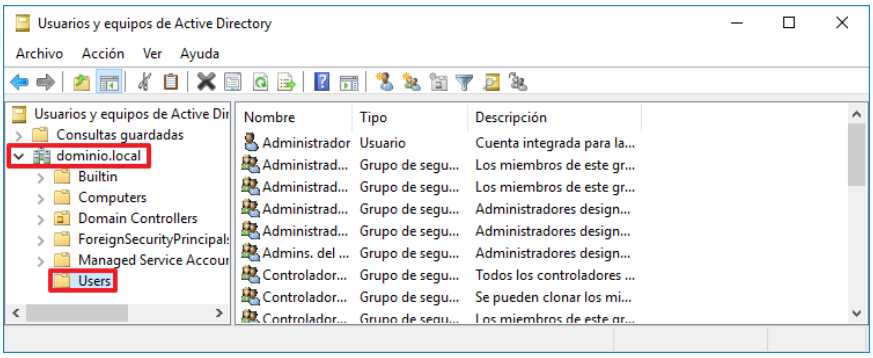
ANEXO A.4.3. GUÍA PASO A PASO SERVIDOR MIEMBRO QUE LE SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA

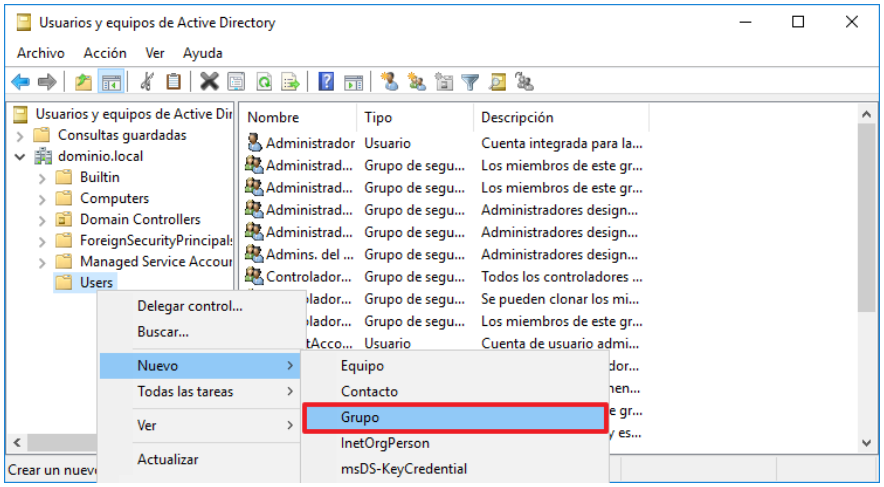
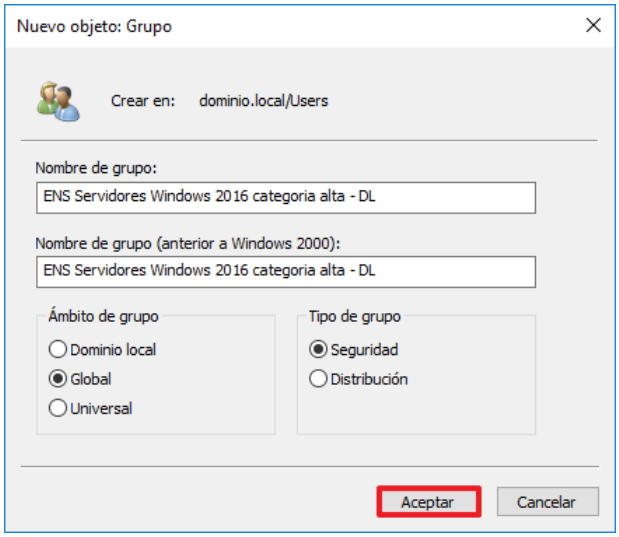
1. PREPARACIÓN DE DOMINIO

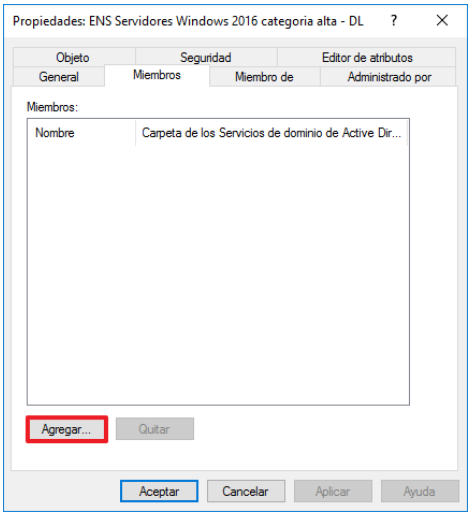
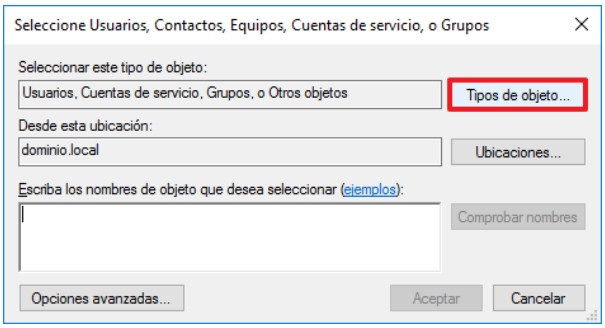
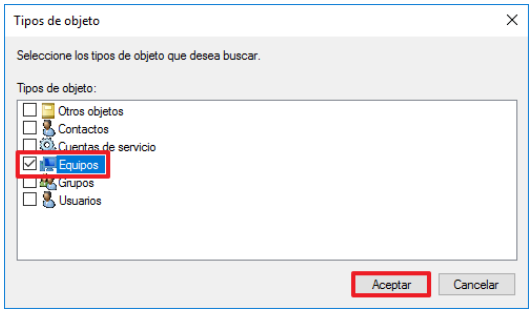
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se realizará la implementación de las plantillas de seguridad. Solo es necesario realizar este procedimiento una vez.

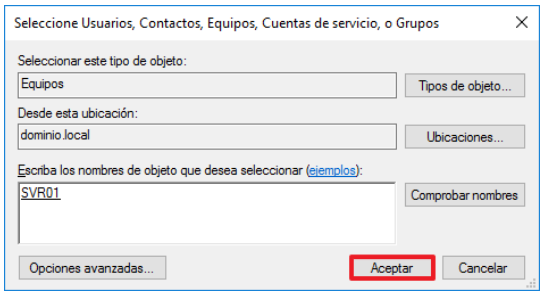
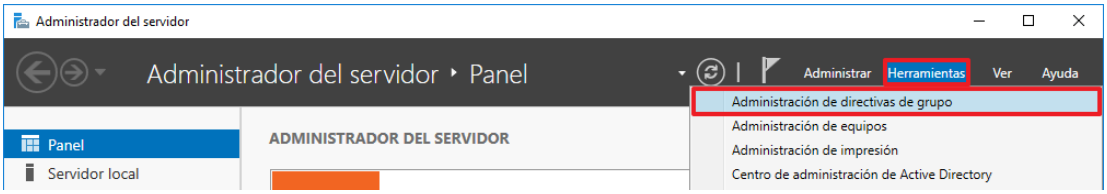
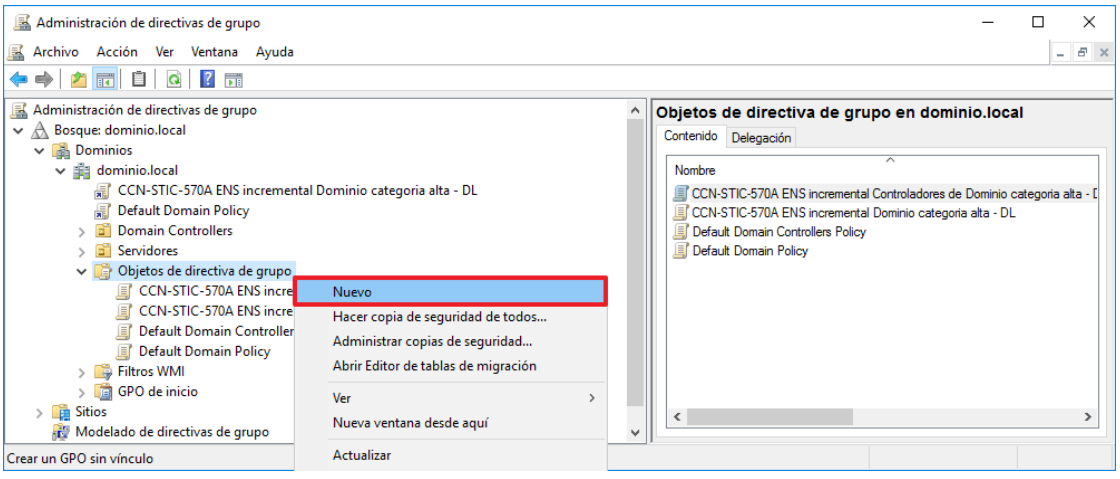
Nota: Esta guía asume que a los servidores controladores del dominio al que va a pertenecer el equipo cliente que está asegurando, se les ha aplicado la configuración descrita en el apartado "ANEXO A.4.1 GUÍA PASO A PASO CONTROLADOR DE DOMINIO QUE LE SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS" de la presente. Si no es así, aplique las configuraciones correspondientes al controlador de dominio, antes de continuar con la aplicación de ésta.

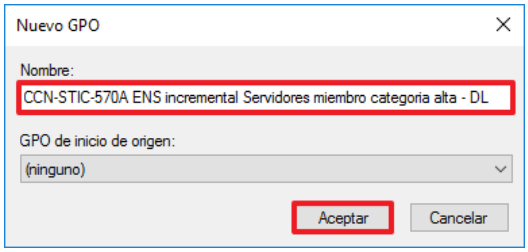
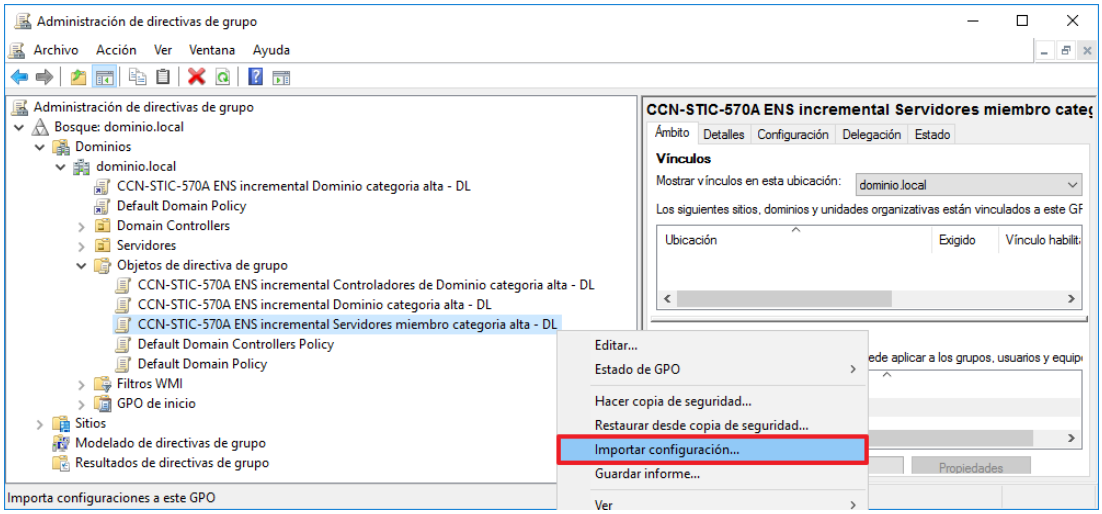
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Cree el directorio "Scripts" en la unidad C:\.
4.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts". **Nota:** Los recursos asociados a esta guía se encuentran en el directorio "Scripts-570A".
5.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio "C:\Scripts" del controlador de dominio: – CCN-STIC-570A ENS servidores categoria alta - DL (directorio) – CCN-STIC-570A ENS incremental DC categoria alta - DL.inf – CCN-STIC-570A ENS incremental dominio categoria alta - DL.inf – CCN-STIC-570A ENS Incremental servidores categoria alta - DL.inf
6.	Copie el fichero "CCN-STIC-570A ENS incremental servidores categoria alta - DL.inf", al directorio "%SYSTEMROOT%\Security\Templates" del Controlador de Dominio. **Nota:** Según la configuración de seguridad de UAC, el sistema podría solicitar la elevación de privilegios, en este caso, pulse "Continuar". 

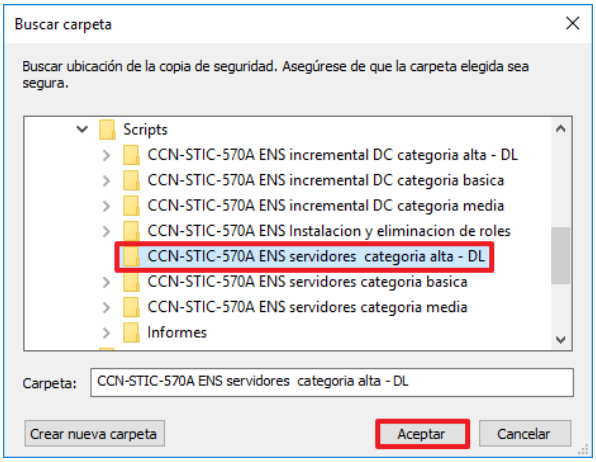
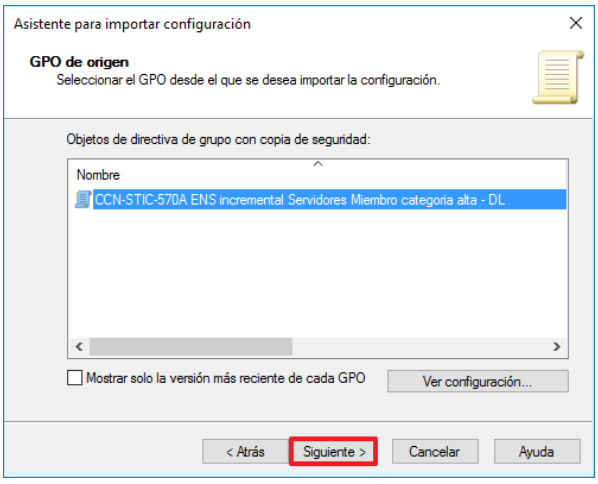
Paso	Descripción
7.	Inicie la herramienta de usuarios y equipos del Directorio Activo. Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Usuarios y equipos de Active Directory"** 
8.	Despliegue el dominio y vaya a la carpeta "Users". 

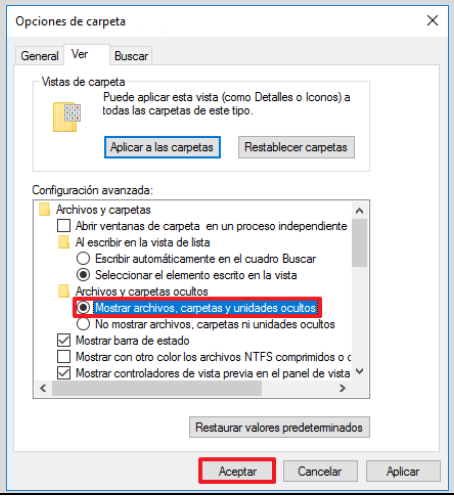
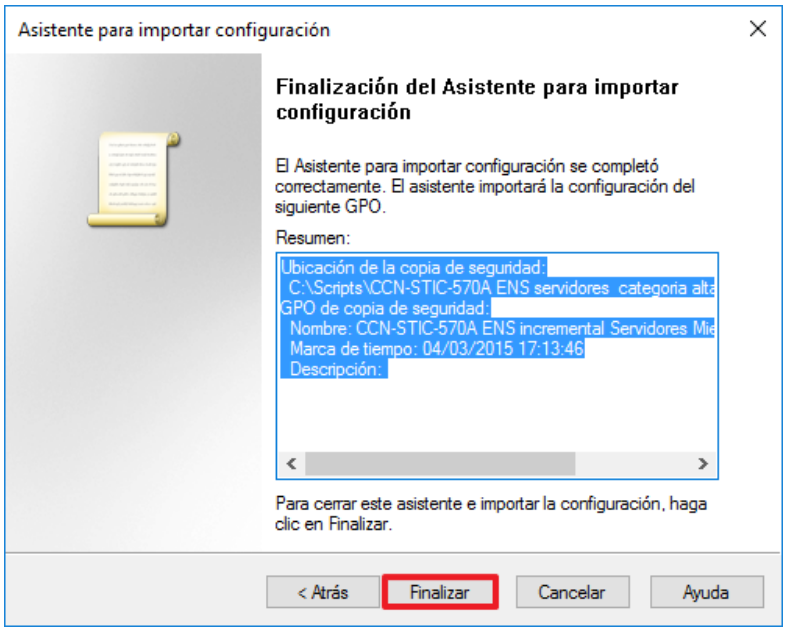
Paso	Descripción
9.	Pulse con el botón derecho sobre dicha carpeta y seleccione la opción **“Nuevo → Grupo”**. 
10.	Introduzca como nombre “ENS servidores Windows 2016 categoria alta - DL”. Deje el resto de opciones como aparecen por defecto y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre servidores miembros del dominio a este grupo creado. 
11.	Abra el nuevo grupo creado pulsando doble clic sobre él y vaya a la pestaña “Miembros”.

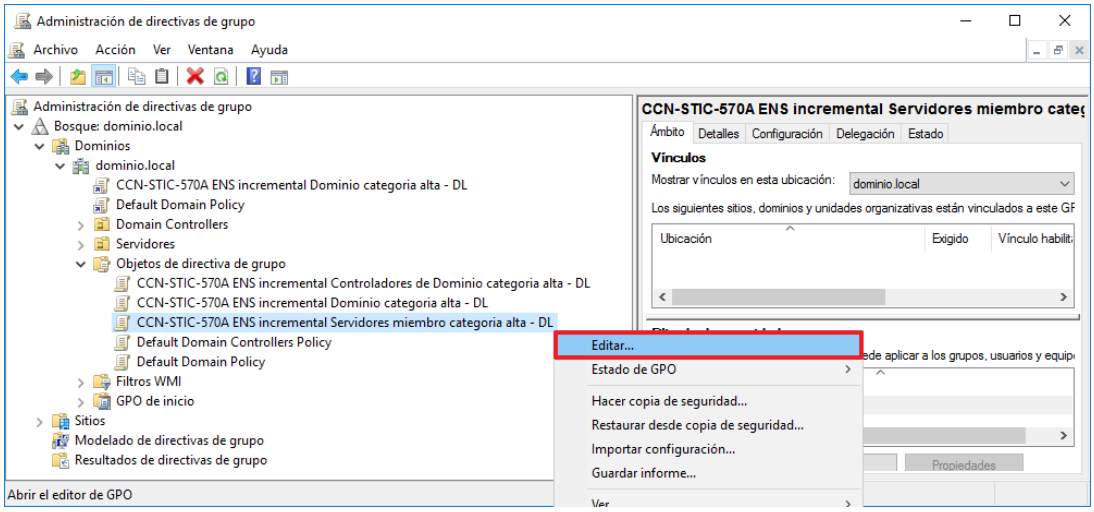
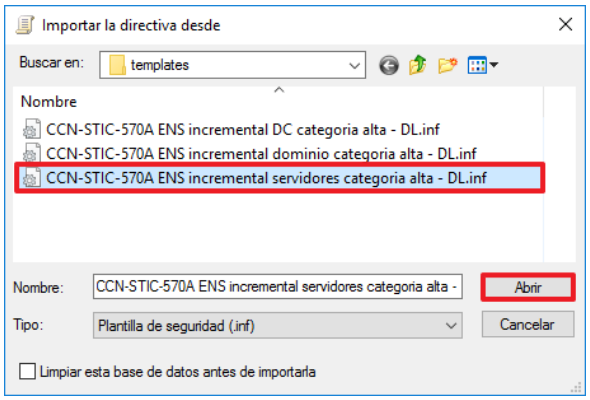
Paso	Descripción
12.	Pulse el botón “Agregar…”. 
13.	Pulse el botón “Tipos de objeto…”. 
14.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 

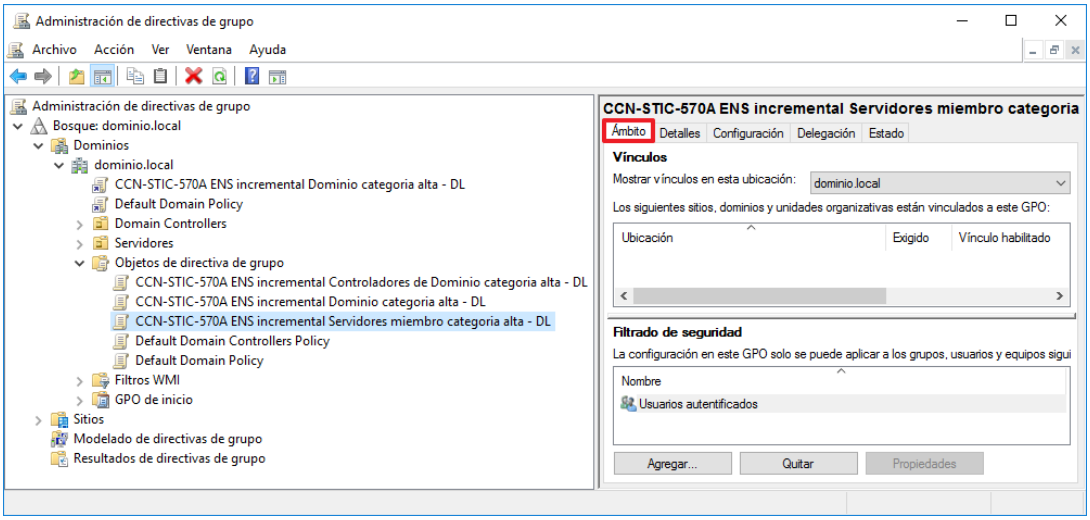
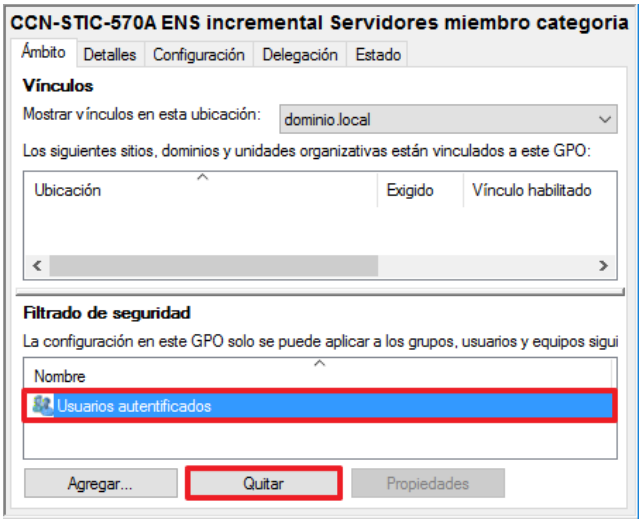
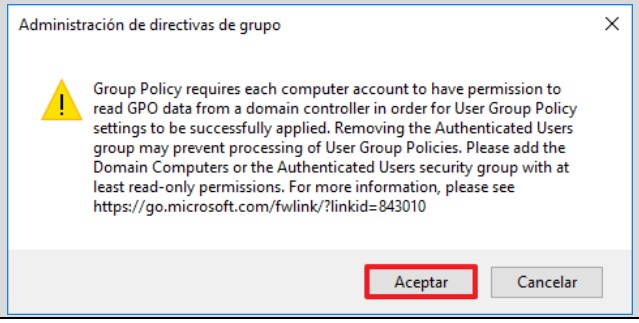
Paso	Descripción
15.	Introduzca el nombre de los servidores o utilice las opciones avanzadas para agregar todos aquellos servidores miembro que se encuentren afectados por el cumplimiento del ENS en su categoría de seguridad alta y pulse el botón “Aceptar”.  **Nota:** No agregue controladores de dominio a este grupo.
16.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo.
17.	Cierre la herramienta de “Usuarios y equipos de Directorio Activo”.
18.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”** 
19.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”.
20.	Pulse con el botón derecho, sobre dicha y carpeta y seleccione la opción “Nuevo”. 

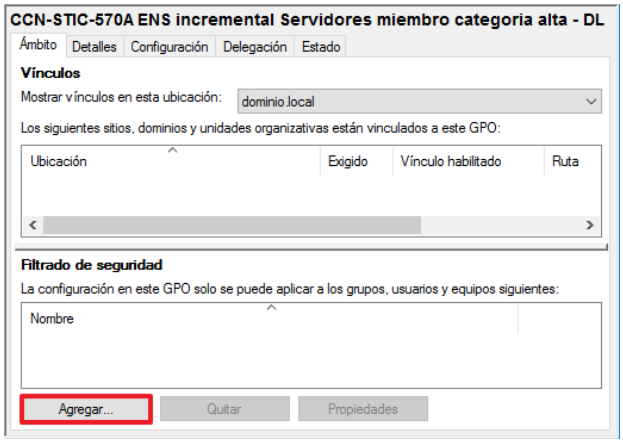
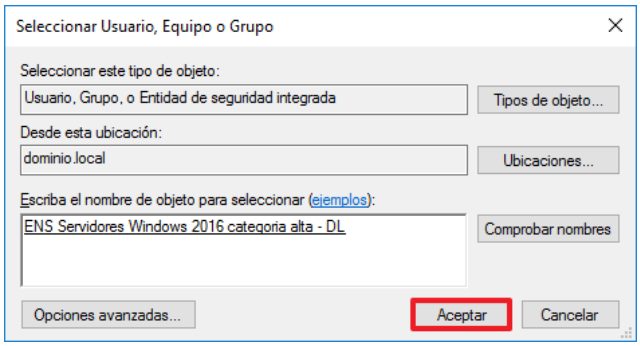
Paso	Descripción
21.	Introduzca como nombre “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL” y pulse el botón “Aceptar”. 
22.	La nueva política requiere una configuración de plantillas administrativas. Para ello y seleccionando la política, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración…”. 
23.	En el asistente de importación de configuración, pulse el botón “Siguiente >”.
24.	En la selección de copia de seguridad, pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.
25.	En la “Carpeta de copia de seguridad”, pulse el botón “Examinar...”.

Paso	Descripción
26.	Seleccione la carpeta “CCN-STIC-570A ENS incremental Servidores categoria alta - DL” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 
27.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada.
28.	En la pantalla siguiente compruebe que aparece la política de seguridad de servidores de categoría alta y pulse el botón “Siguiente >”. 

Paso	Descripción
	Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero "manifest.xml". Este es un fichero oculto y, por lo tanto, debe mostrar en "opciones de carpeta", la opción "Mostrar archivos, carpetas y unidades ocultos". 
29.	En la pantalla de examen, pulse el botón "Siguiente >".
30.	Si apareciera la ventana "Migrar referencias", mantenga las opciones y pulse el botón "Siguiente >".
31.	Para completar el asistente pulse el botón "Finalizar". 
32.	Pulse el botón "Aceptar" para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración.

Paso	Descripción
33.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
34.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**
35.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva…”.
36.	Seleccione de la ruta “C:\Windows\Security\Templates” el fichero “CCN-STIC-570A ENS incremental servidores categoria alta - DL” y pulse el botón “Abrir”. 
37.	Cierre la política de grupo.

Paso	Descripción
38.	Seleccione la nueva política de grupo configurada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 
39.	De la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
40.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. **Nota:** En caso de que aparezca la siguiente advertencia ignórela y pulse “Aceptar”. 

Paso	Descripción
41.	Una vez quitado, pulse el botón “Agregar…”. 
42.	Introduzca como nombre “ENS servidores Windows 2016 categoria alta - DL”. Este grupo corresponde con el generado en pasos previos. A continuación, pulse el botón “Aceptar”. 
43.	Las políticas se encuentran ya creadas correctamente. No obstante, no se aplicarán hasta más adelante, una vez que haya tenido en cuenta y aplicado todas las consideraciones adicionales que se mostrarán en el siguiente punto del presente anexo. Cierre la herramienta “Administración de Directivas de Grupo”.

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

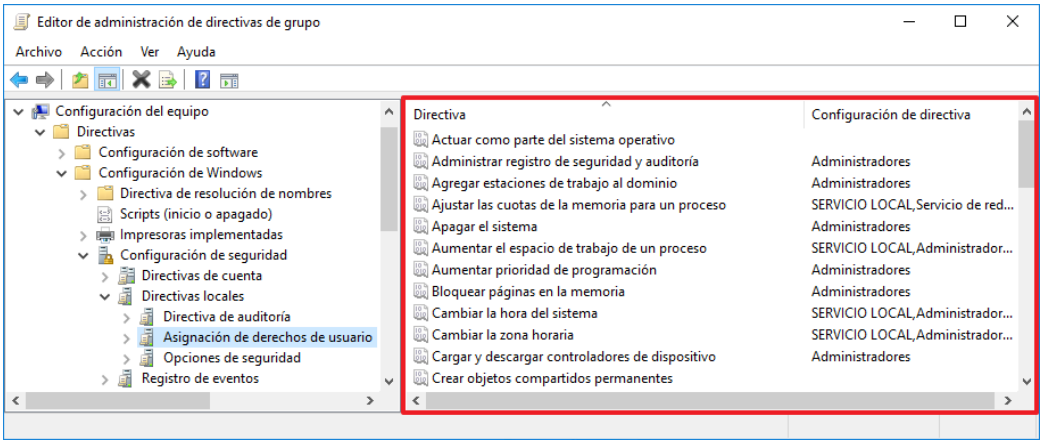
El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración. Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría alta. No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

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

2.1. ASIGNACIÓN DE DERECHOS DE USUARIO

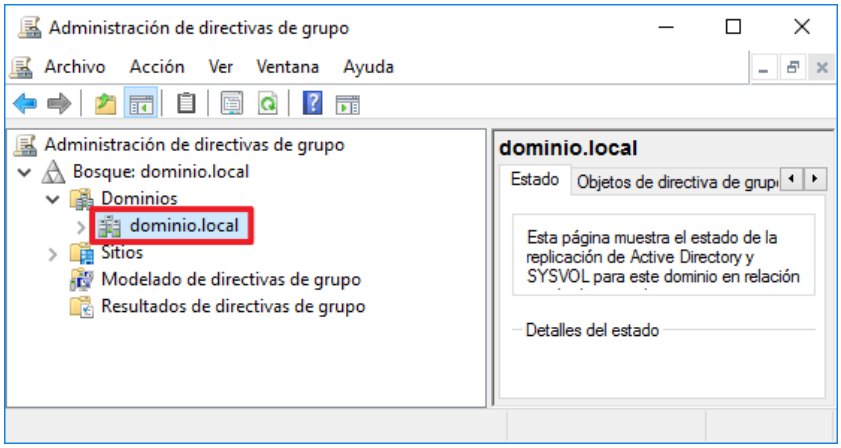
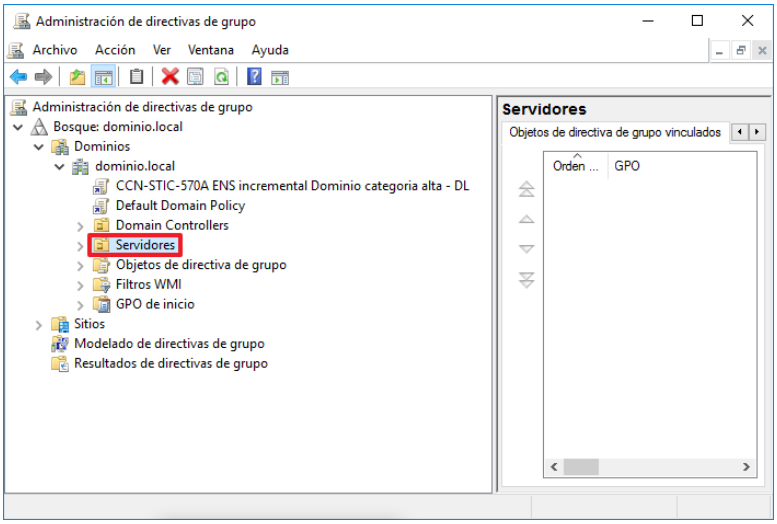
Los objetos de políticas de grupo para Controladores de Dominio y Servidores miembros especifican unos derechos de usuario siguiendo planteamientos de seguridad que aplican los principios de mínimo privilegio y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les hayan asignado derechos determinados para la administración o gestión de los sistemas.

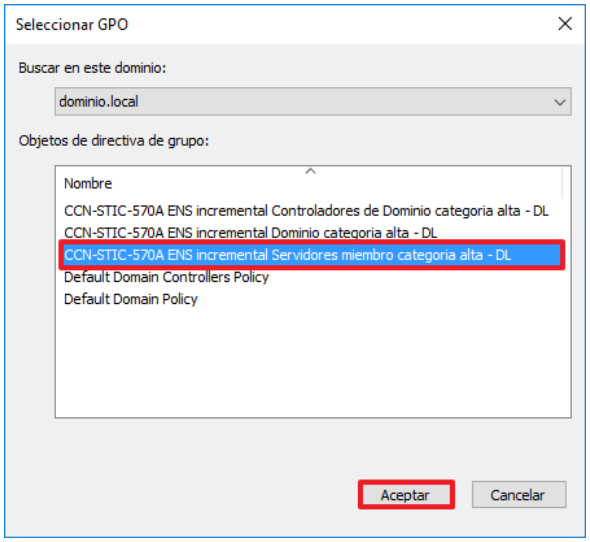
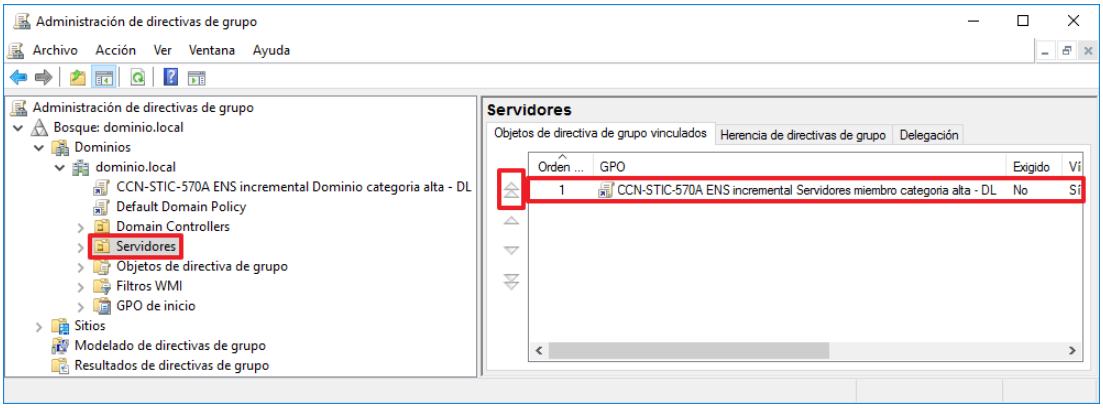
Si esto fuera así, deberá realizar las modificaciones pertinentes sobre el objeto de política de grupo "CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL".

Paso	Descripción
44.	Edite la política de grupo correspondiente iniciando la herramienta "Administración de Directivas de Grupo" y seleccionando la política a modificar. Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"** Sobre el objeto de GPO que se quiere modificar, deberá pulsar clic derecho y seleccionar "Editar" en el menú desplegado.
45.	Una vez abierto el "Editor de administración de directivas de grupo", despliegue la política y sitúese en la siguiente ruta: **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"** 
46.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
47.	Guarde la configuración cerrando la ventana de editor de administración de directivas de grupo.

3. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

El presente punto establece la aplicación de las políticas de seguridad, toda vez que se han tenido en consideración las condiciones definidas en el punto previo.

Paso	Descripción
48.	Inicie la herramienta de administración de directivas de grupo.
49.	Despliegue el bloque y posiciónese sobre su dominio.  **Nota:** En el ejemplo el dominio utilizado se denomina “dominio.local”.
50.	Identifique las ubicaciones donde se encuentran los servidores Windows Server 2016 que les son de aplicación las condiciones de seguridad de categoría alta, según estipula el ENS. Sobre cada una de esas ubicaciones, asigne el objeto de política de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL”.  **Nota:** En el ejemplo se aplicará sobre la OU “Servidores”, que es donde se encuentran ubicados los servidores analizados en el escenario de test.
51.	Pulse con el botón derecho del ratón sobre la unidad organizativa correspondiente y selecciones la opción “Vincular un objeto GPO existente…”.

Paso	Descripción
52.	Seleccione la política “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL” y pulse el botón “Aceptar”. 
53.	Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL” y pulse el botón con la flecha que apunta hacia arriba hasta situarla en primer lugar dentro del orden de vínculo. 
54.	Repita los pasos 49 a 53 en cada una de las unidades organizativas donde se encuentren los servidores miembro Windows Server 2016 sujetos al cumplimiento del ENS en su categoría alta.
55.	Cierre la herramienta de administración de directivas de grupo.
56.	Elimine la carpeta “C:\Scripts”.

4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD EN LOS EQUIPOS

Las configuraciones planteadas a través de la presente guía han sido ampliamente probadas en entornos de operativa Microsoft. No obstante, no se han podido probar todas las condiciones existentes, ni con las peculiaridades de cada organización. Bajo determinadas condiciones, pudieran suceder algunas incidencias que se describen a continuación, así como su resolución.

Debe tenerse en consideración que la resolución consiste en rebajar algunos de los mecanismos de seguridad descritos en la presente guía. Por lo tanto, deberá plantearse una solución que, de forma paulatina, permita alcanzar el estado de seguridad deseado y recomendado por la presente guía.

4.1. CONTROL DE CUENTAS DE USUARIO

El control de cuentas de usuario surge en Windows Vista como respuesta para limitar las acciones de los administradores cuando actuaban con cuentas privilegiadas ante acciones que no requieren dicho privilegio. En sistemas previos a Windows Vista, un administrador que había iniciado una sesión actuaba siempre con los máximos privilegios, independientemente de que estuviera abriendo un fichero ofimático o estuviera navegando por internet. Puesto que el riesgo era bastante elevado, Microsoft propuso como solución UAC, con objeto de advertir a los administradores cuando una acción requería privilegio para actuar.

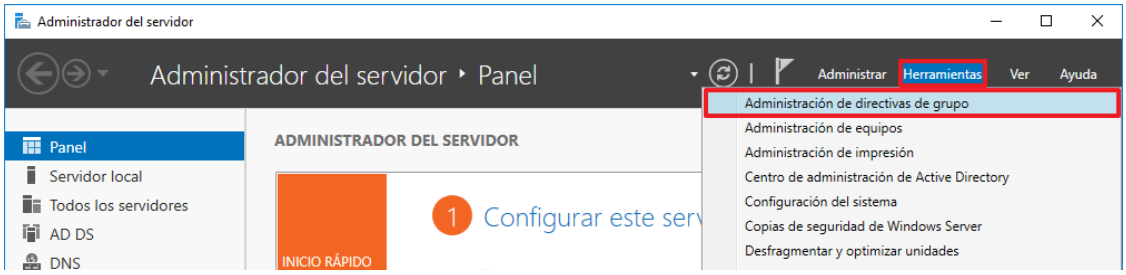
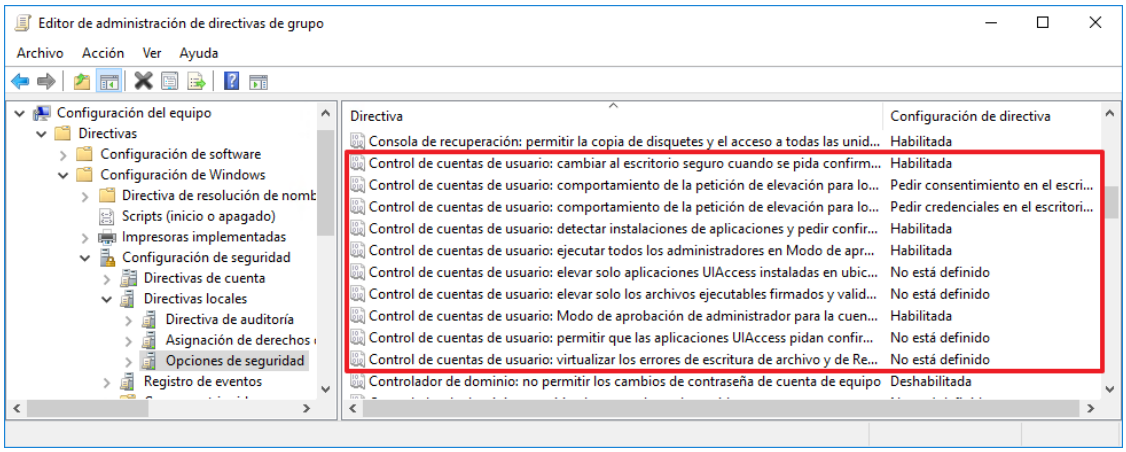
Siguiendo el principio de menor privilegio y menor exposición, la presente guía habilita las condiciones de funcionalidad de UAC para la categoría alta, aunque con los criterios más laxos de los aplicables.

No obstante, y ante aplicaciones o servicios antiguos, pudieran darse fallos de funcionalidad en los mismos requiriendo que se realicen análisis o la modificación en la configuración de UAC predeterminada para la categoría alta por la presente guía.

Los siguientes pasos definen los procedimientos para la creación de una nueva política de seguridad de aplicación a los servidores que pudieran presentar incidencias con una nueva política de seguridad para el UAC.

Nota: La modificación deberá afectar exclusivamente a servidores miembro. Los controladores de dominio no deberían tener problemas en la ejecución de todos sus servicios en el modo de UAC habilitado.

Paso	Descripción
57.	Identifique los servidores que tienen problemas para la ejecución de aplicaciones y servicios y quítelos como miembros del grupo “ENS servidores Windows 2016 categoria alta - DL”.
58.	Cree un nuevo grupo con nombre “ENS servidores miembro 2016 categoria alta - DL incidencias UAC”, e incluya en dicho grupo los servidores miembro con una categoría alta que presenten incidencias de funcionalidad del UAC. Realice estas tareas siguiendo los pasos 7 a 17 del presente anexo.

Paso	Descripción
59.	Inicie la herramienta de “Administración de directivas de grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Inicio → Herramientas Administrativas → Administración de directivas de grupo”** 
60.	Cree una nueva política de grupo con el nombre “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL incidencias UAC”. Siga, para ello, los pasos 18 a 37 de este anexo. A continuación vincule el objeto de política de grupo a la unidad organizativa correspondiente siguiendo los pasos 48 a 55 de este anexo.
61.	Adicionalmente, asigne la nueva política de grupo al grupo de servidores recién creado “ENS servidores miembro 2016 categoria alta - DL incidencias UAC”. Siga, para ello, los pasos 38 a 42 de este anexo.
62.	Edite el nuevo objeto de GPO “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL incidencias UAC”. Para ello seleccione dicha política y seleccione la opción “Editar…”.
63.	Despliegue la política y sitúese en la siguiente ruta: **“Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**
64.	Identifique las directivas relativas a “Control de cuenta de usuario”. 
65.	Realice las modificaciones oportunas.
66.	Cierre la política.

Paso	Descripción
67.	Para que la nueva política sea efectiva, necesita reiniciar el o los servidores. Esto es debido a que la aplicación se basa en la membresía a un grupo. La condición del miembro del grupo es adquirida por un equipo cuando inicia sesión en el dominio, cuestión que se produce cuando el equipo se reinicia. **Nota:** Debe tener en consideración que, si ha alterado la política de Control de cuentas de usuario y ésta es menos rigurosa que la propuesta en la configuración deseada por esta guía, se encuentra por debajo de los requerimientos de seguridad actuales. Debería evaluar los problemas ocasionados por las aplicaciones y servicios e intentar adaptarlos a configuraciones válidas. Es factible que si los servicios y/o aplicaciones no presentan funcionalidad con UAC presenten riesgos de seguridad notables y se esté exponiendo de forma significativa la infraestructura de la organización.

ANEXO A.4.4. LISTA DE COMPROBACIÓN DE WINDOWS SERVER 2016 COMO SERVIDOR MIEMBRO DE DOMINIO PARA LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía "ANEXO A.4.3 GUÍA PASO A PASO SERVIDOR MIEMBRO QUE LE SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS".

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los dominios y servidores Windows Server 2016 con implementación de seguridad de categoría alta del ENS.

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

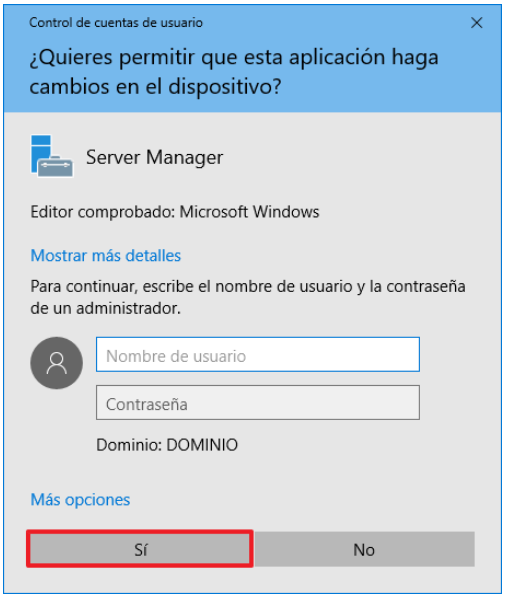
a) Administrador del Servidor.

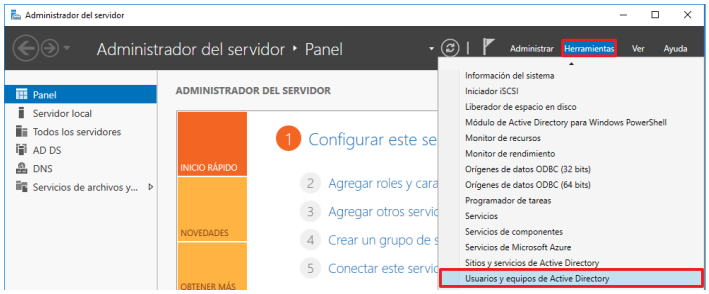
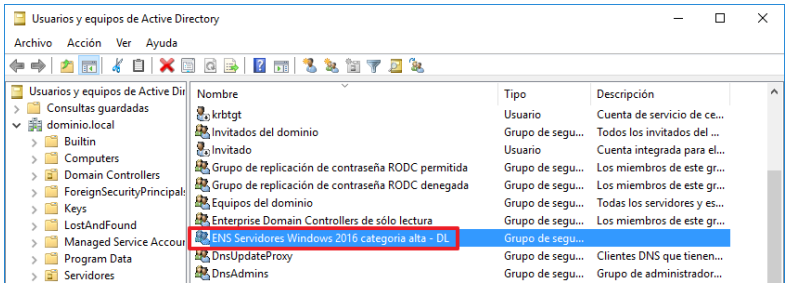
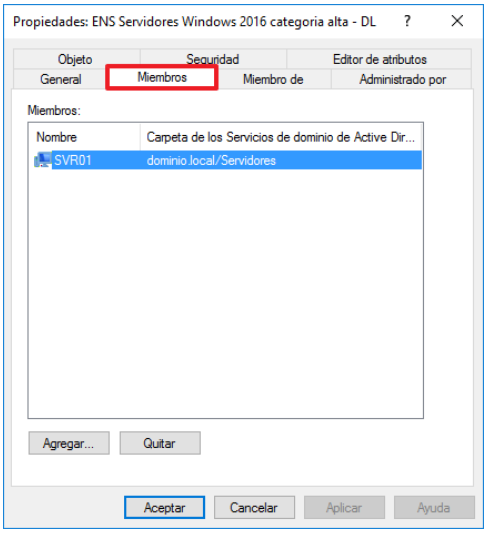
b) Conjunto resultante de directivas (rsop.msc).

c) Consola de servicios (services.msc).

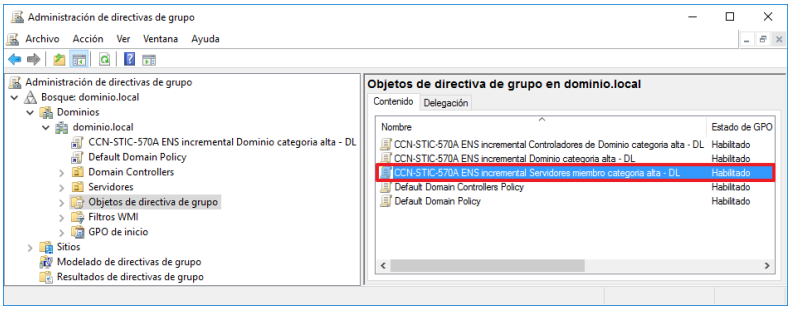
d) Editor de registro (regedit.exe).

e) Explorador de Archivos (explorer.exe).

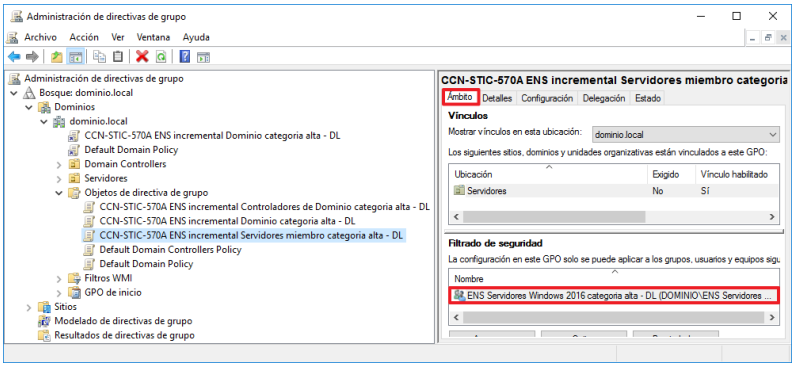
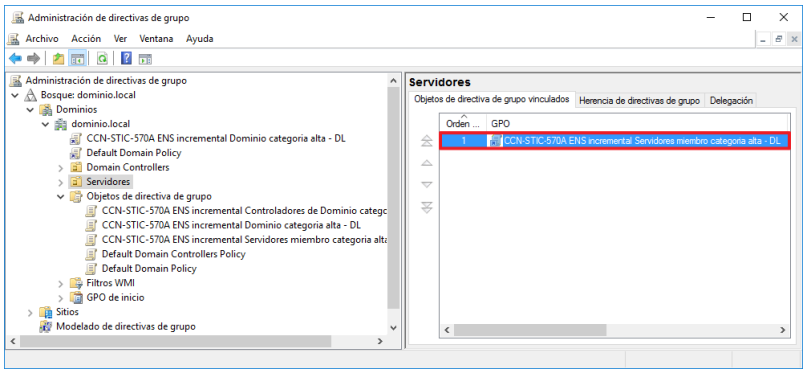
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el servidor controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Pulse "Sí" en la ventana de "Control de cuentas de usuario". 

Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que está creado el grupo “ENS servidores Windows 2016 categoría alta” dentro del contenedor “Users”.		Ejecute la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  Seleccione el contenedor “Users”, situado en la siguiente ruta: “**Usuarios y equipos de Active Directory → [Su dominio] → Users**” A continuación, en el panel de la derecha, verifique que está creado el objeto denominado “ENS servidores Windows 2016 categoria alta - DL”. 
3. Verifique que los servidores que han sido catalogados como de categoría de seguridad alta y siguiendo los criterios definidos en el ENS, son miembros del grupo “ENS servidores Windows 2016 categoria alta - DL”.		Pulse doble clic sobre el grupo “ENS servidores Windows 2016 categoria alta - DL” situado en el panel de la derecha y seleccione la pestaña “Miembros” para verificar que los servidores que corresponden a esta categoría de seguridad aparecen en el listado. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>4. Verifique que los objetos de directivas de grupo han sido creados y están habilitados.</td><td></td><td>Ejecute la herramienta “Administrador de directivas de grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione:
“Herramientas → Administración de directivas de grupo”
 

Dentro de la consola diríjase a los “Objetos de directiva de grupo”:
“Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo”
Verifique que está creado el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL” y que en la columna “Estado de GPO” figuran como habilitada.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL</td><td>Habilitado</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
5. Verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL” tiene definido el Ámbito al grupo “ENS servidores Windows 2016 categoria alta - DL”		En el árbol de la izquierda, pulse doble clic sobre el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL” desde: **“Bosques [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo”** Verifique en la pestaña “Ámbito” que dentro del campo “Filtrado de seguridad” figura el grupo “ENS servidores Windows 2016 categoria alta - DL”. 
6. Verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL” aplica a todos los objetos de las OU con servidores correspondientes a la categoría alta según los criterios del ENS y ocupa el primer lugar en el orden de vinculación.		En el árbol de la izquierda sitúese sobre las unidades organizativas con servidores correspondientes a la categoría alta según los criterios del ENS, en el ejemplo, “Servidores” desde: **“Bosque: [Su bosque] → Dominios → [Su Dominio] → Servidores”** En la pestaña “Objetos de Directiva de grupo vinculados” verifique que el objeto de directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL” figura en el panel de la derecha y ocupa el primer lugar en la columna “Orden de Vínculos”. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>7. Verifique los valores de auditoría de la directiva de grupo “CCN-STIC-570A ENS incremental servidores miembro categoria alta - DL”.</td><td></td><td>En el “Administrador de Directivas de Grupo” de uno de los controladores del dominio, pulse el botón derecho del ratón sobre la directiva desde:
“Bosque: [Su Bosque] → Dominios → [Su Dominio] → [OU de servidores] → CCN-STIC-570A ENS incremental servidores miembro categoria alta - DL”
Seleccione la opción “Editar…”. Cuando se abra el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Auditar el acceso a objetos</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar el acceso del servicio de directorio</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar el cambio de directivas</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar el seguimiento de procesos</td><td>Sin auditoría</td><td></td></tr>
<tr><td>Auditar el uso de privilegios</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar eventos de inicio de sesión</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar eventos de inicio de sesión de cuenta</td><td>Correcto, Erróneo</td><td></td></tr>
<tr><td>Auditar eventos del sistema</td><td>Correcto</td><td></td></tr>
<tr><td>Auditar la administración de cuentas</td><td>Correcto, Erróneo</td><td></td></tr>
</table></td></tr>
<tr><td>8. Verifique los valores de asignación de derechos de usuario en la directiva de grupo “CCN-STIC-570A ENS incremental servidores miembro categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Administrar registro de seguridad y auditoría	Administradores	
		Agregar estaciones de trabajo al dominio	Administradores	
		Ajustar las cuotas de la memoria para un proceso	Administradores, SERVICIO LOCAL, Servicio de red	
		Apagar el sistema	Administradores	
		Aumentar el espacio de trabajo de un proceso	Administradores, SERVICIO LOCAL	
		Aumentar prioridad de programación	Administradores	
		Bloquear páginas en la memoria	Administradores	
		Cambiar la hora del sistema	SERVICIO LOCAL, Administradores	
		Cambiar la zona horaria	SERVICIO LOCAL, Administradores	
		Cargar y descargar controladores de dispositivo	Administradores	
		Crear Objetos globales	Administradores, SERVICIO, SERVICIO LOCAL, Servicio de red	
		Crear un archivo de paginación	Administradores	
		Crear vínculos simbólicos	Administradores	
		Denegar el acceso desde la red a este equipo	ANONYMOUS LOGON, Invitados	
		Denegar el inicio de sesión como servicio	Invitados	
		Denegar el inicio de sesión como trabajo por lotes	Invitados	
		Denegar el inicio de sesión local	Invitados	
		Denegar el inicio de sesión a través de Servicios de Escritorio Remoto	Invitados	
		Forzar cierre desde un sistema remoto	Administradores	
		Generar auditorías de seguridad	SERVICIO LOCAL, Servicio de red	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Generar perfiles de un solo proceso	Administradores	
		Generar perfiles de rendimiento del sistema	Administradores	
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	Administradores	
		Hacer copias de seguridad de archivos y directorios	Administradores, Operadores de copia de seguridad	
		Modificar la etiqueta de un objeto	Administradores	
		Modificar valores de entorno firmware	Administradores	
		Permitir el inicio de sesión local	Administradores	
		Quitar equipo de la estación de acoplamiento	Administradores	
		Realizar tareas de mantenimiento de volumen	Administradores	
		Reemplazar un símbolo (token) de nivel de proceso	SERVICIO LOCAL, Servicio de red	
		Restaurar archivos y directorios	Administradores	
		Suplantar a un cliente tras la autenticación	Administradores, SERVICIO, SERVICIO LOCAL, Servicio de red	
		Tener acceso a este equipo desde la red	Administradores, Usuarios autentificados, ENTERPRISE DOMAIN CONTROLLERS	
		Tomar posesión de archivos y otros objetos	Administradores	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>9. Verifique los valores de las opciones de seguridad de la directiva de grupo “CCN-STIC-570A ENS incremental servidores miembro categoria alta-DL”</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de Seguridad”</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Acceso a redes: modelo de seguridad y uso compartido para cuentas locales</td><td>Clásico: usuarios locales se autentican con credenciales propias</td><td></td></tr>
<tr><td>Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos</td><td>Deshabilitada</td><td></td></tr>
<tr><td>Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos</td><td>Habilitada</td><td></td></tr>
<tr><td>Acceso a redes: rutas del Registro accesibles remotamente</td><td>System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, Software\Microsoft\Windows NT\CurrentVersion</td><td></td></tr>
</table>
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Acceso a redes: rutas y subrutas del Registro accesibles remotamente	Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib, System\CurrentControlSet\Services\SysmonLog	
		Acceso de red: permitir traducción SID/nombre anónima	Deshabilitada	
		Apagado: borrar el archivo de paginación de la memoria virtual	Habilitada	
		Apagado: permitir apagar el sistema sin tener que iniciar sesión	Deshabilitada	
		Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad	Habilitada	
		Directiva	Valor	OK/NOK

Comprobación	OK/NOK	Cómo hacerlo		
		Auditoría: auditar el acceso de objetos globales del sistema	Habilitada	
		Auditoría: auditar el uso del privilegio de copias de seguridad y restauración	Habilitada	
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitada	
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitada	
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada	
		Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitada	
		Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitada	
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitada	
		Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador	Pedir credenciales en el escritorio seguro	
		Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar	Pedir credenciales en el escritorio seguro	
		Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación	Habilitada	
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitada	
	Directiva		**Valor**	**OK/NOK**
	Control de cuentas de usuario:		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo	
	elevar solo aplicaciones UIAccess instaladas en ubicaciones seguras		
	Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitada	
	Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitada	
	Control de cuentas de usuario: Virtualizar los errores de escritura de archivo y de Registro en diferentes ubicaciones por usuario	Habilitada	
	Controlador de dominio: no permitir los cambios de contraseña de cuenta de equipo	Deshabilitada	
	Controlador de dominio: permitir a los operadores de servidor programar tareas	Deshabilitada	
	Controlador de dominio: requisitos de firma de servidor LDAP	Requerir firma	
	Criptografía de sistema: forzar la protección con claves seguras para las claves de usuario almacenadas en el equipo	El usuario debe escribir una contraseña cada vez que use una clave	
	Cirptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash	Habilitada	
	Cuentas: estado de la cuenta de invitado	Deshabilitada	
	Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitada	

	Directiva	Valor	OK/NOK
	DCOM: restricciones de acceso al equipo en sintaxis de Lenguaje de definición de	O:BAG:BAD: (A;;CCDCLC;;;AU)(A;;CCDCLC;;;S-1-5-32-562)	

Comprobación	OK/NOK	Cómo hacerlo	
	descriptores de seguridad (SDDL)		
	DCOM: restricciones de inicio al equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)	O:BAG:BAD: (A;;CCDCLCSWRP;;;BA)(A;;CCDCSW;;;AU)(A;;CCDCLCSWRP;;;S-1-5-32-562)	
	Dispositivos: impedir que los usuarios instalen controladores de impresora	Habilitada	
	Dispositivos: Permitir desacoplamiento sin tener que iniciar sesión	Deshabilitada	
	Dispositivos: permitir formatear y expulsar medios extraíbles	Administradores	
	Dispositivos: restringir el acceso a disquetes sólo al usuario con sesión iniciada localmente	Habilitada	
	Dispositivos: restringir el acceso al CD-ROM sólo al usuario con sesión iniciada localmente	Habilitada	
	Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo	
	Inicio de sesión interactivo: mostrar información de usuario cuando se bloquee la sesión	No mostrar la información del usuario	
	Inicio de sesión interactivo: no mostrar el último nombre de usuario	Habilitada	
	Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr	Deshabilitada	
	Inicio de sesión interactivo: número de inicios de sesión anteriores que se almacenarán en caché (si el controlador de dominio no está disponible	0 inicios de sesión	
	Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire	14 días	

	Directiva	Valor	OK/NOK
	Inicio de sesión interactivo: requerir la autenticación del Controlador de Dominio para desbloquear la estación de	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo	
	trabajo		
	Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	
	Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitada	
	Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitada	
	Miembro de dominio: duración máxima de contraseña de cuenta de equipo	30 días	
	Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	
	Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitada	
	Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitada	
	Seguridad de red: nivel de autenticación de LAN Manager	Enviar sólo respuesta NTLMv2 y rechazar LM	
	Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada	
	Seguridad de red: permitir que LocalSystem use la identidad del equipo para NTLM	Habilitada	
	Seguridad de red: permitir retroceso a sesión NULL de LocalSystem	Deshabilitada	

Directiva	Valor	OK/NOK
Seguridad de red: permitir solicitudes de autenticación PKU2U a este equipo para usar identidades en Internet	Deshabilitada	
Seguridad de red: requisitos de firma de cliente LDAP	Requerir firma	

Comprobación	OK/NOK	Cómo hacerlo	
	Seguridad de red: restringir NTLM: auditar el tráfico NTLM entrante	Habilitar la auditoría para todas las cuentas	
	Seguridad de red: restringir NTLM: auditar la autenticación NTLM en este dominio	Habilitar todo	
	Seguridad de red: restringir NTLM: autenticación NTLM en este dominio	Denegar para cuentas de dominio en servidores de dominio	
	Seguridad de red: restringir NTLM: tráfico NTLM entrante	Denegar todas las cuentas de dominio	
	Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)	Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits	
	Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)	Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits	
	Servidor de red Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitada	
	Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitada	
	Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada	
	Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor	Requerido del cliente	
	Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión	15 minutos	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>10. Verifique el registro de eventos de la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro de eventos”</td></tr>
<tr><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Evitar que el grupo de invitados locales tenga acceso al registro de aplicaciones</td><td>Habilitada</td><td></td></tr>
<tr><td>Evitar que el grupo de invitados locales tenga acceso al registro de seguridad</td><td>Habilitada</td><td></td></tr>
<tr><td>Evitar que el grupo de invitados locales tenga acceso al registro del sistema</td><td>Habilitada</td><td></td></tr>
<tr><td>Método de retención del registro de la aplicación</td><td>Según se necesite</td><td></td></tr>
<tr><td>Método de retención del registro de seguridad</td><td>Según se necesite</td><td></td></tr>
<tr><td>Método de retención del registro del sistema</td><td>Según se necesite</td><td></td></tr>
<tr><td>Tamaño máximo del registro de la aplicación</td><td>32768 kilobytes</td><td></td></tr>
<tr><td>Tamaño máximo del registro de seguridad</td><td>163840 kilobytes</td><td></td></tr>
<tr><td>Tamaño máximo del registro del sistema</td><td>32768 kilobytes</td><td></td></tr>
</table></td></tr>
<tr><td>11. Verifique los servicios de sistema en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”

Nota: Dependiendo de los servicios que estén instalados en el equipo, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales (antivirus, etc.).
En la siguiente tabla se muestran el nombre largo y el nombre corto para cada servicio. En la ventana del editor de administración de directivas de grupo sólo aparecerá uno de los dos: el nombre largo si el servicio está instalado en el sistema o el nombre corto si no lo está.
Además, deberá tener en cuenta que los números existentes en algunos servicios son aleatorios y cambian en cada equipo.</td></tr>
<tr><td colspan="3"><table>
<tr><th>Servicio (nombre largo)</th><th>Servicio (nombre corto)</th><th>Inicio</th><th>Permiso</th><th>OK/NOK</th></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo			
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado		
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado		
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado		
Administración de aplicaciones	AppMgmt	Manual	Configurado		
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado		
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado		
Administración remota de Windows (WS-Management)	WinRM	Automático	Configurado		
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado		
Administrador de conexiones de acceso remoto	RasMan	Manual	Configurado		
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado		
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado		
Administrador de credenciales	VaultSvc	Manual	Configurado		
Administrador de cuentas de seguridad	SamSs	Automático	Configurado		
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado		
Administrador de sesión local	LSM	Automático	Configurado		
Administrador de usuarios	UserManager	Automático	Configurado		
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**	
Agente de conexión de	NcbService	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
red					
Agente de detección en segundo plano de DevQuery		DevQueryBroker	Manual	Configurado	
Agente de directiva IPsec		PolicyAgent	Manual	Configurado	
Agente de eventos de tiempo		TimeBrokerSvc	Manual	Configurado	
Agente de eventos del sistema		SystemEventsBroker	Automático	Configurado	
Aislamiento de claves CNG		KeyIso	Manual	Configurado	
Almacenamiento de datos de usuarios		UnistoreSvc	Manual	Configurado	
Aplicación auxiliar de NetBIOS sobre TCP/IP		lmhosts	Manual	Configurado	
Aplicación auxiliar IP		iphlpsvc	Automático	Configurado	
Aplicación del sistema COM+		COMSysApp	Manual	Configurado	
Archivos sin conexión		CscService	Deshabilitado	Configurado	
Asignador de detección de topologías de nivel de vínculo		lltdsvc	Manual	Configurado	
Asignador de extremos de RPC		RpcEptMapper	Automático	Configurado	
Asistente para la conectividad de red		NcaSvc	Manual	Configurado	
Audio de Windows		Audiosrv	Manual	Configurado	
Ayuda del Panel de control de Informes de problemas y soluciones		wercplsupport	Deshabilitado	Configurado	
Ayudante especial de la consola de administración		sacsvr	Manual	Configurado	
Ayudante para el inicio de sesión de cuenta Microsoft		wlidsvc	Manual	Configurado	
Captura SNMP		SNMPTRAP	Deshabilitado	Configurado	
CDPUserSvc		CDPUserSvc	Automático	Configurado	
Cliente de directiva de grupo		gpsvc	Automático	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Cliente de seguimiento de vínculos distribuidos		TrkWks	Automático	Configurado	
Cliente DHCP		Dhcp	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Cliente DNS		Dnscache	Automático	Configurado	
Cola de impresión		Spooler	Automático	Configurado	
Compilador de extremo de audio de Windows		AudioEndpointBuilder	Manual	Configurado	
Conexión compartida a Internet (ICS)		SharedAccess	Deshabilitado	Configurado	
Conexiones de red		Netman	Manual	Configurado	
Configuración automática de redes cableadas		dot3svc	Manual	Configurado	
Configuración de Escritorio remoto		SessionEnv	Manual	Configurado	
Conjunto resultante de proveedor de directivas		RSoPProv	Manual	Configurado	
Contenedor de Microsoft Passport		NgcCtnrSvc	Manual	Configurado	
Coordinador de transacciones distribuidas		MSDTC	Automático	Configurado	
CoreMessaging		CoreMessagingRegistrar	Automático	Configurado	
DataCollectionPublishingService		DcpSvc	Manual	Configurado	
Datos de contactos		PimIndexMaintenanceSvc	Manual	Configurado	
Detección de hardware shell		ShellHWDetection	Deshabilitado	Configurado	
Detección de servicios interactivos		UI0Detect	Manual	Configurado	
Detección SSDP		SSDPSRV	Deshabilitado	Configurado	
Directiva de extracción de tarjetas inteligentes		SCPolicySvc	Manual	Configurado	
Disco virtual		vds	Manual	Configurado	
Dispositivo host de UPnP		upnphost	Manual	Configurado	
DLL de host del Contador de rendimiento		PerfHost	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
dmwappushsvc		dmwappushservice	Deshabilitado	Configurado	
Energía		Power	Automático	Configurado	
Enrutamiento y acceso remoto		RemoteAccess	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Estación de trabajo	LanmanWorkstation	Automático	Configurado		
Eventos de adquisición de imágenes estáticas	WiaRpc	Manual	Configurado		
Examinador de equipos	Browser	Deshabilitado	Configurado		
Experiencia de calidad de audio y vídeo de Windows (qWave)	QWAVE	Deshabilitado	Configurado		
Extensiones y notificaciones de impresora	PrintNotify	Manual	Configurado		
Firewall de Windows	MpsSvc	Automático	Configurado		
Hora de Windows	W32Time	Automático	Configurado		
Host de proveedor de detección de función	fdPHost	Deshabilitado	Configurado		
Host de sistema de diagnóstico	WdiSystemHost	Deshabilitado	Configurado		
Host del servicio de diagnóstico	WdiServiceHost	Deshabilitado	Configurado		
Identidad de aplicación	AppIDSvc	Manual	Configurado		
Información de la aplicación	Appinfo	Manual	Configurado		
Iniciador de procesos de servidor DCOM	DcomLaunch	Automático	Configurado		
Inicio de sesión secundario	seclogon	Deshabilitado	Configurado		
Instalador de ActiveX (AxInstSV)	AxInstSV	Manual	Configurado		
Instalador de módulos de Windows	TrustedInstaller	Manual	Configurado		
Instantáneas de volumen	VSS	Manual	Configurado		
Instrumental de administración de Windows	Winmgmt	Automático	Configurado		
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
KTMRM para DTC (Coordinador de transacciones distribuidas)	KtmRm	Manual	Configurado	
Llamada a procedimiento remoto (RPC)	RpcSs	Automático	Configurado	
Microsoft App-V Client	AppVClient	Deshabilitado	Configurado	
Microsoft Passport	NgcSvc	Manual	Configurado	
Modo incrustado	embeddedmode	Manual	Configurado	
Módulos de creación de claves de IPsec para IKE y AuthIP	IKEEXT	Manual	Configurado	
Motor de filtrado de base	BFE	Automático	Configurado	
Net Logon	Netlogon	Automático	Configurado	
Optimizar unidades	defragsvc	Manual	Configurado	
Partida guardada en Xbox Live	XblGameSave	Deshabilitado	Configurado	
Plug and Play	PlugPlay	Manual	Configurado	
Preparación de aplicaciones	AppReadiness	Manual	Configurado	
Programador de tareas	Schedule	Automático	Configurado	
Propagación de certificados	CertPropSvc	Manual	Configurado	
Protección de software	sppsvc	Automático	Configurado	
Protocolo de autenticación extensible	Eaphost	Manual	Configurado	
Proveedor de instantáneas de software de Microsoft	swprv	Manual	Configurado	
Publicación de recurso de detección de función	FDResPub	Deshabilitado	Configurado	
Reconoc. ubicación de red	NlaSvc	Automático	Configurado	
Recopilador de eventos de Windows	Wecsvc	Manual	Configurado	
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Registro de eventos de Windows	EventLog	Automático	Configurado	
Registro remoto	RemoteRegistry	Deshabilitado	Configurado	
Registros y alertas de rendimiento	pla	Manual	Configurado	
Servicio Asistente para la compatibilidad de programas	PcaSvc	Automático	Configurado	
Servicio biométrico de Windows	WbioSrvc	Manual	Configurado	
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc	Manual	Configurado	
Servicio de administración de aplicaciones de empresa	EntAppSvc	Manual	Configurado	
Servicio de administración de radio	RmSvc	Manual	Configurado	
Servicio de administrador de licencias de Windows	LicenseManager	Manual	Configurado	
Servicio de almacenamiento	StorSvc	Manual	Configurado	
Servicio de asociación de dispositivos	DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows	FontCache	Deshabilitado	Configurado	
Servicio de cierre de invitado de Hyper-V	vmicshutdown	Manual	Configurado	
Servicio de compatibilidad con Bluetooth	bthserv	Manual	Configurado	
Servicio de configuración de red	NetSetupSvc	Manual	Configurado	
Servicio de datos del sensor	SensorDataService	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP	WinHttpAutoProxySvc	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**

Comprobación	OK/NOK	Cómo hacerlo			
Servicio de directivas de diagnóstico	DPS	Deshabilitado	Configurado		
Servicio de dispositivo de interfaz humana	hidserv	Manual	Configurado		
Servicio de enrutador de AllJoyn	AJRouter	Deshabilitado	Configurado		
Servicio de enumeración de dispositivos de tarjeta inteligente	ScDeviceEnum	Manual	Configurado		
Servicio de geolocalización	lfsvc	Manual	Configurado		
Servicio de host HV	HvHost	Manual	Configurado		
Servicio de implementación de AppX (AppXSVC)	AppXSvc	Manual	Configurado		
Servicio de infraestructura de tareas en segundo plano	BrokerInfrastructure	Automático	Configurado		
Servicio de inscripción de administración de dispositivos	DmEnrollmentSvc	Manual	Configurado		
Servicio de inspección de red de Windows Defender	WdNisSvc	Manual	Configurado		
Servicio de instalación de dispositivos	DeviceInstall	Manual	Configurado		
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado		
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado		
Servicio de licencia de cliente (ClipSVC)	ClipSVC	Manual	Configurado		
Servicio de lista de redes	netprofm	Manual	Configurado		
Servicio de notificación de eventos de sistema	SENS	Automático	Configurado		
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService	Deshabilitado	Configurado		
Servicio de perfil de usuario	ProfSvc	Automático	Configurado		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**	
Servicio de plataforma	CDPSvc	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
de dispositivos conectados					
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Manual	Configurado		
Servicio de puerta de enlace de nivel de aplicación	ALG	Manual	Configurado		
Servicio de registro de acceso de usuarios	UALSVC	Automático	Configurado		
Servicio de repositorio de estado	StateRepository	Manual	Configurado		
Servicio de sensores	SensorService	Manual	Configurado		
Servicio de servidor proxy KDC (KPS)	KPSSVC	Manual	Configurado		
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado		
Servicio de supervisión de licencias de Windows	WLMS	Automático	Configurado		
Servicio de supervisión de sensores	SensrSvc	Manual	Configurado		
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Manual	Configurado		
Servicio de uso compartido de datos	DsSvc	Manual	Configurado		
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Deshabilitado	Configurado		
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Manual	Configurado		
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual	Configurado		
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**	
Servicio de Windows Defender	WinDefend	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio de Windows Insider	wisvc	Manual	Configurado	
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado	
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Manual	Configurado	
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado	
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Manual	Configurado	
Servicio FrameServer de la Cámara de Windows	FrameServer	Manual	Configurado	
Servicio host de proveedor de cifrado de Windows	WEPHOSTSVC	Manual	Configurado	
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado	
Servicio Interfaz de almacenamiento en red	nsi	Automático	Configurado	
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado	
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standardcollector.service	Manual	Configurado	
Servicio telefónico	PhoneSvc	Manual	Configurado	
Servicios de cifrado	CryptSvc	Automático	Configurado	
Servicios de Escritorio remoto	TermService	Manual	Configurado	
Servidor	LanmanServer	Automático	Configurado	
Servidor del modelo de datos del mosaico	tiledatamodelsvc	Automático	Configurado	
Sincronizar host	OneSyncSvc	Automático	Configurado	
Sistema de cifrado de archivos (EFS)	EFS	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Sistema de eventos COM+	EventSystem	Automático	Configurado	
SMP de Espacios de	smphost	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
almacenamiento de Microsoft				
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado	
Superfetch	SysMain	Manual	Configurado	
Tarjeta inteligente	SCardSvr	Deshabilitado	Configurado	
Telefonía	TapiSrv	Deshabilitado	Configurado	
Telemetría y experiencias del usuario conectado	DiagTrack	Automático	Configurado	
Temas	Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)	RpcLocator	Manual	Configurado	
WalletService	WalletService	Manual	Configurado	
Windows Driver Foundation - User-mode Driver Framework	wudfsvc	Manual	Configurado	
Windows Installer	msiserver	Manual	Configurado	
Windows Search	WSearch	Deshabilitado	Configurado	
Windows Update	wuauserv	Manual	Configurado	
SMP de Espacios de almacenamiento de Microsoft	smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado	
Superfetch	SysMain	Manual	Configurado	
Tarjeta inteligente	SCardSvr	Deshabilitado	Configurado	
Telefonía	TapiSrv	Deshabilitado	Configurado	
Telemetría y experiencias del usuario conectado	DiagTrack	Automático	Configurado	
Temas	Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)	RpcLocator	Manual	Configurado	
WalletService	WalletService	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Windows Driver Foundation - User-mode Driver Framework	wudfsvc	Manual	Configurado	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="4">Cómo hacerlo</th></tr>
<tr><td colspan="2">Windows Installer</td><td>msiserver</td><td>Manual</td><td>Configurado</td><td></td></tr>
<tr><td rowspan="3">12. Verifique los permisos de valores de registro de la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL”.</td><td></td><td colspan="4">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro”

Nota: Para verificar los permisos de la entrada de registro, deberá pulsar doble clic sobre la entrada “MACHINES → SOFTWARE → Microsoft → Windows → CurrentVersion → Installer” y pulsar sobre el botón "Modificar seguridad...".
Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".</td></tr>
<tr><td colspan="2">Directiva</td><td colspan="2">Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer</td><td colspan="2">Administradores: Control Total
SYSTEM: Control Total
Usuarios: Leer</td><td></td></tr>
<tr><td>13. Verifique los valores del sistema de archivos de la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL”.</td><td></td><td colspan="4">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de Archivos”

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

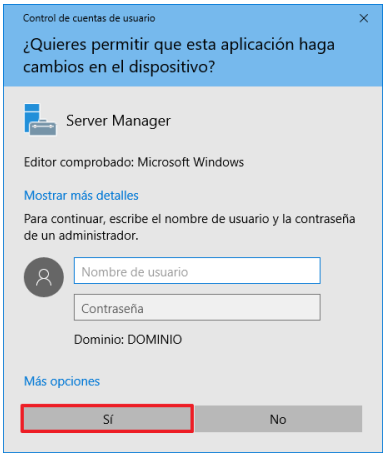
Comprobación	OK/NOK	Cómo hacerlo		
Archivo		**Usuario**	**Permiso**	**OK/NOK**
%SystemRoot%\Registration		Administrador	Control total	
		System	Control total	
		Usuario	Leer y ejecutar	
%SystemRoot%\repair		Administrador	Control total	
		System	Control total	
%SystemRoot%\security		Administrador	Control total	
		System	Control total	
SystemRoot%\system32\cacls		Administrador	Control total	
		System	Control total	
SystemRoot%\system32\clip.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\ras		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\rasadhlp.dll		Administrador	Control total	
%SystemRoot%\system32\rasauto.dll		Administrador	Control total	
%SystemRoot%\system32\rasautou.exe		Administrador	Control total	
%SystemRoot%\system32\raschap.dll		Administrador	Control total	
%SystemRoot%\system32\rasctrnm.h		Administrador	Control total	
%SystemRoot%\system32\rasctrs.dll		Administrador	Control total	
%SystemRoot%\system32\rasctrs.ini		Administrador	Control total	
%SystemRoot%\system32\rasdial		Administrador	Control total	
%SystemRoot%\system32\rasmans.dll		Administrador	Control total	
%SystemRoot%\system32\rasmontr.dll		Administrador	Control total	
%SystemRoot%\system32\rasphone.exe		Administrador	Control total	
%SystemRoot%\system32\rasppp.dll		Administrador	Control total	
%SystemRoot%\system32\rastapi.dll		Administrador	Control total	
%SystemRoot%\system32\rastls.dll		Administrador	Control total	
%SystemRoot%\system32\runonce.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\secedit.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\telnet.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\tftp.exe		Administrador	Control total	
		System	Control total	
%SystemRoot%\system32\tracert.exe		Administrador	Control total	
		System	Control total	

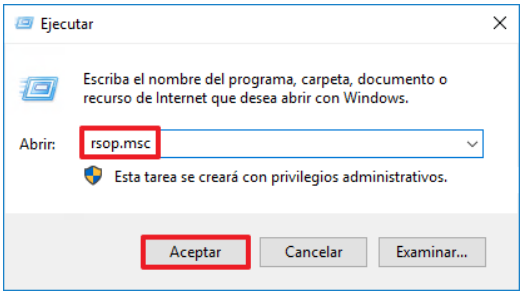
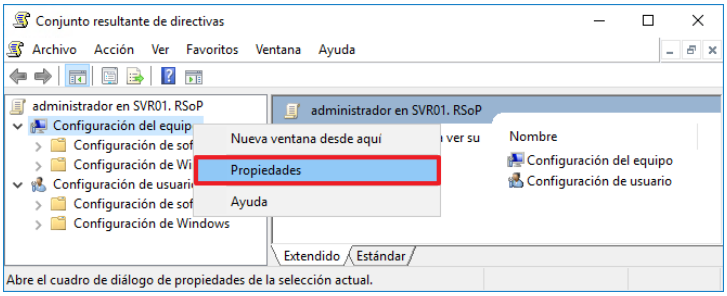
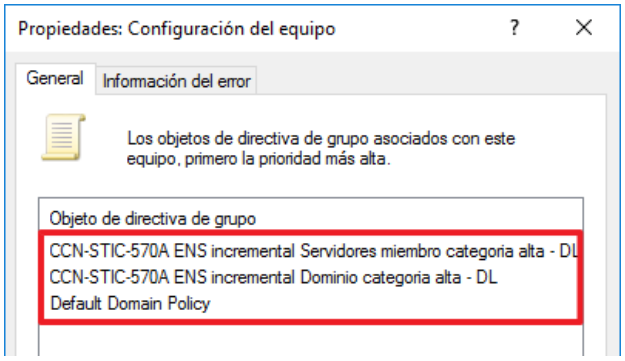
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td rowspan="3">14. Verifique que está bloqueada la ejecución del Almacén digital en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Administración de derechos digitales de Windows Media”</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Impedir el acceso a internet de Windows Media DRM</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="3">15. Verifique que está bloqueada la ejecución del Almacén digital en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Almacén Digital”</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>No permitir que se ejecute el Almacén digital</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td></td><td></td></tr>
</table>

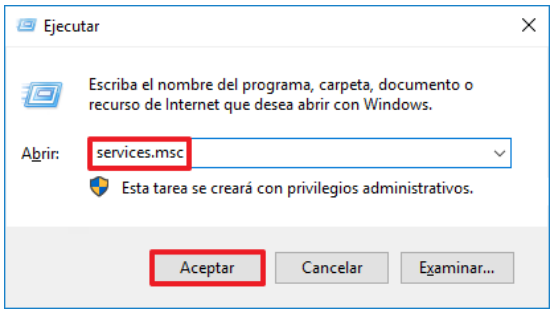
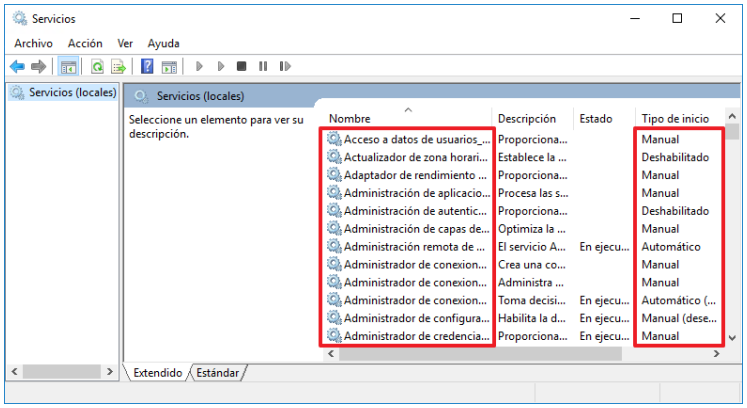
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>16. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Biometría”</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Permitir el uso de biometría</td><td>Habilitada</td><td></td></tr>
<tr><td>Permitir que los usuarios de dominio inicien sesión mediante biometría</td><td>Habilitada</td><td></td></tr>
<tr><td>Permitir que los usuarios inicien sesión mediante biometría</td><td>Habilitada</td><td></td></tr>
</table>
</td></tr>
<tr><td>17. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Directivas de reproducción automática”</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Desactivar reproducción automática</td><td>Habilitada</td><td></td></tr>
<tr><td>Establecer el comportamiento predeterminado para ejecución automática.</td><td>Habilitada</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td rowspan="4">18. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL”.</td><td></td><td colspan="2">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Informe de errores de Windows”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Deshabilitar el informe de errores de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">No enviar datos adicionales</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="4">19. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL”.</td><td></td><td colspan="2">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Opciones de inicio de sesión de Windows”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Informar cuando el servidor de inicio de sesión no está disponible durante el inicio de sesión del usuario</td><td>Habilitada</td><td></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>20. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Componentes de Windows → Shell remoto de Windows”</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Permitir acceso a Shell remoto</td><td>Deshabilitada</td><td></td></tr>
</table>
</td></tr>
<tr><td>21. Verifique configuración de la comunicación de Internet en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Desactivar informe de errores de reconocimiento de escritura a mano</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el Programa para la mejora de la experiencia del usuario de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar los vínculos “Events.asp” del Visor de eventos</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el contenido “¿Sabía que…?” del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la búsqueda en Microsoft Knowledge Base del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Desactivar el informe de errores de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la actualización de archivos de contenido del Asistente para búsqueda</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el acceso a la Tienda</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar la tarea de imágenes “Pedir copias fotográficas”</td><td>Habilitada</td><td></td></tr>
<tr><td>Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td rowspan="2">22. Verifique los valores de “Informe de errores de Windows” en la directiva de grupo “CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL”.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Plantillas administrativas: definiciones de directiva (archivos ADMX) recuperadas del equipo local. → Sistema → Net Logon”</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Permitir algoritmos de criptografía compatibles con Windows NT 4.0</td><td>Deshabilitada</td><td></td></tr>
</table></td></tr>
<tr><td>23. Inicie sesión en el servidor a comprobar.</td><td></td><td>Inicie sesión con una cuenta que tenga privilegios de administración del dominio en el servidor a comprobar.
El sistema solicitará elevación de privilegios para poder ejecutar el “Administrador del Servidor”. Pulse “Sí” en la ventana de “Control de cuentas de usuario”
 
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
24. Verifique que el equipo ha recibido la directiva de grupo CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL.		Ejecute la consola de administración "Conjunto resultante de directivas" (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → rsop.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" en la ventana que se muestra a continuación:  Seleccione en ella la rama "Configuración del equipo", márquela con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la figura:  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", resaltada en la siguiente figura:  Verifique que en dicha sección aparecen listados, y por ese orden, los objetos de directiva de grupo que se indican en la siguiente tabla:

Comprobación	OK/NOK	Cómo hacerlo
	Objeto de directiva de grupo	OK/NOK
	CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL	
	CCN-STIC-570A ENS incremental Dominio categoria alta - DL	
	Default Domain Policy	
25. Verifique que los servicios del sistema están correctamente configurados		Usando la consola de servicios (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → services.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" para continuar.  Verifique que el tipo de inicio de los servicios que aparecen en el sistema y en la siguiente tabla coinciden:  **Nota:** Dependiendo del equipo, es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales (antivirus, etc.).

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado	
Administración de aplicaciones	AppMgmt	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado	
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado	
Administración remota de Windows (WS-Management)	WinRM	Automático	Configurado	
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado	
Administrador de conexiones de acceso remoto	RasMan	Manual	Configurado	
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado	
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado	
Administrador de credenciales	VaultSvc	Manual	Configurado	
Administrador de cuentas de seguridad	SamSs	Automático	Configurado	
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado	
Administrador de sesión local	LSM	Automático	Configurado	
Administrador de usuarios	UserManager	Automático	Configurado	
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado	
Agente de conexión de red	NcbService	Manual	Configurado	
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado	
Agente de directiva IPsec	PolicyAgent	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Agente de eventos de	TimeBrokerSvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
tiempo					
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado		
Aislamiento de claves CNG	KeyIso	Manual	Configurado		
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado		
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado		
Aplicación auxiliar IP	iphlpsvc	Automático	Configurado		
Aplicación del sistema COM+	COMSysApp	Manual	Configurado		
Archivos sin conexión	CscService	Deshabilitado	Configurado		
Asignador de detección de topologías de nivel de vínculo	lltdsvc	Manual	Configurado		
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado		
Asistente para la conectividad de red	NcaSvc	Manual	Configurado		
Audio de Windows	Audiosrv	Manual	Configurado		
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Deshabilitado	Configurado		
Ayudante especial de la consola de administración	sacsvr	Manual	Configurado		
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado		
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado		
CDPUserSvc	CDPUserSvc	Automático	Configurado		
Cliente de directiva de grupo	gpsvc	Automático	Configurado		
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático	Configurado		
Cliente DHCP	Dhcp	Automático	Configurado		
Cliente DNS	Dnscache	Automático	Configurado		
Cola de impresión	Spooler	Automático	Configurado		
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Manual	Configurado		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**	
Comprobador puntual	svsvc	Manual	Configurado		
Conexión compartida a	SharedAccess	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Internet (ICS)					
Conexiones de red		Netman	Manual	Configurado	
Configuración automática de redes cableadas		dot3svc	Manual	Configurado	
Configuración de Escritorio remoto		SessionEnv	Manual	Configurado	
Conjunto resultante de proveedor de directivas		RSoPProv	Manual	Configurado	
Contenedor de Microsoft Passport		NgcCtnrSvc	Manual	Configurado	
Coordinador de transacciones distribuidas		MSDTC	Automático	Configurado	
CoreMessaging		CoreMessagingRegistrar	Automático	Configurado	
DataCollectionPublishingService		DcpSvc	Manual	Configurado	
Datos de contactos		PimIndexMaintenanceSvc	Manual	Configurado	
Detección de hardware shell		ShellHWDetection	Deshabilitado	Configurado	
Detección de servicios interactivos		UI0Detect	Manual	Configurado	
Detección SSDP		SSDPSRV	Deshabilitado	Configurado	
Directiva de extracción de tarjetas inteligentes		SCPolicySvc	Manual	Configurado	
Disco virtual		vds	Manual	Configurado	
Dispositivo host de UPnP		upnphost	Manual	Configurado	
DLL de host del Contador de rendimiento		PerfHost	Manual	Configurado	
dmwappushsvc		dmwappushservice	Deshabilitado	Configurado	
Energía		Power	Automático	Configurado	
Enrutamiento y acceso remoto		RemoteAccess	Deshabilitado	Configurado	
Estación de trabajo		LanmanWorkstation	Automático	Configurado	
Eventos de adquisición de imágenes estáticas		WiaRpc	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Examinador de equipos		Browser	Deshabilitado	Configurado	
Experiencia de calidad de audio y vídeo de		QWAVE	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Windows (qWave)					
Extensiones y notificaciones de impresora		PrintNotify	Manual	Configurado	
Firewall de Windows		MpsSvc	Automático	Configurado	
Hora de Windows		W32Time	Automático	Configurado	
Host de proveedor de detección de función		fdPHost	Deshabilitado	Configurado	
Host de sistema de diagnóstico		WdiSystemHost	Deshabilitado	Configurado	
Host del servicio de diagnóstico		WdiServiceHost	Deshabilitado	Configurado	
Identidad de aplicación		AppIDSvc	Manual	Configurado	
Información de la aplicación		Appinfo	Manual	Configurado	
Iniciador de procesos de servidor DCOM		DcomLaunch	Automático	Configurado	
Inicio de sesión secundario		seclogon	Deshabilitado	Configurado	
Instalador de ActiveX (AxInstSV)		AxInstSV	Manual	Configurado	
Instalador de módulos de Windows		TrustedInstaller	Manual	Configurado	
Instantáneas de volumen		VSS	Manual	Configurado	
Instrumental de administración de Windows		Winmgmt	Automático	Configurado	
Interfaz de servicio invitado de Hyper-V		vmicguestinterface	Manual	Configurado	
KTMRM para DTC (Coordinador de transacciones distribuidas)		KtmRm	Manual	Configurado	
Llamada a procedimiento remoto (RPC)		RpcSs	Automático	Configurado	
Microsoft App-V Client		AppVClient	Deshabilitado	Configurado	
Microsoft Passport		NgcSvc	Manual	Configurado	
Modo incrustado		embeddedmode	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Módulos de creación de claves de IPsec para IKE y AuthIP		IKEEXT	Manual	Configurado	
Motor de filtrado de		BFE	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
base					
Net Logon		Netlogon	Automático	Configurado	
Optimizar unidades		defragsvc	Manual	Configurado	
Partida guardada en Xbox Live		XblGameSave	Deshabilitado	Configurado	
Plug and Play		PlugPlay	Manual	Configurado	
Preparación de aplicaciones		AppReadiness	Manual	Configurado	
Programador de tareas		Schedule	Automático	Configurado	
Propagación de certificados		CertPropSvc	Manual	Configurado	
Protección de software		sppsvc	Automático	Configurado	
Protocolo de autenticación extensible		Eaphost	Manual	Configurado	
Proveedor de instantáneas de software de Microsoft		swprv	Manual	Configurado	
Publicación de recurso de detección de función		FDResPub	Deshabilitado	Configurado	
Reconoc. ubicación de red		NlaSvc	Automático	Configurado	
Recopilador de eventos de Windows		Wecsvc	Manual	Configurado	
Redirector de puerto en modo usuario de Servicios de Escritorio remoto		UmRdpService	Manual	Configurado	
Registro de eventos de Windows		EventLog	Automático	Configurado	
Registro remoto		RemoteRegistry	Deshabilitado	Configurado	
Registros y alertas de rendimiento		pla	Manual	Configurado	
Servicio Asistente para la compatibilidad de programas		PcaSvc	Automático	Configurado	
Servicio biométrico de Windows		WbioSrvc	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de actualizaciones Orchestrator para Windows Update		UsoSvc	Manual	Configurado	
Servicio de		EntAppSvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
administración de aplicaciones de empresa					
Servicio de administración de radio		RmSvc	Manual	Configurado	
Servicio de administrador de licencias de Windows		LicenseManager	Manual	Configurado	
Servicio de almacenamiento		StorSvc	Manual	Configurado	
Servicio de asociación de dispositivos		DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows		FontCache	Deshabilitado	Configurado	
Servicio de cierre de invitado de Hyper-V		vmicshutdown	Manual	Configurado	
Servicio de compatibilidad con Bluetooth		bthserv	Manual	Configurado	
Servicio de configuración de red		NetSetupSvc	Manual	Configurado	
Servicio de datos del sensor		SensorDataService	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP		WinHttpAutoProxySvc	Manual	Configurado	
Servicio de directivas de diagnóstico		DPS	Deshabilitado	Configurado	
Servicio de dispositivo de interfaz humana		hidserv	Manual	Configurado	
Servicio de enrutador de AllJoyn		AJRouter	Deshabilitado	Configurado	
Servicio de enumeración de dispositivos de tarjeta inteligente		ScDeviceEnum	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de geolocalización		lfsvc	Manual	Configurado	
Servicio de host HV		HvHost	Manual	Configurado	
Servicio de implementación de AppX (AppXSVC)		AppXSvc	Manual	Configurado	
Servicio de		BrokerInfrastructure	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
infraestructura de tareas en segundo plano					
Servicio de inscripción de administración de dispositivos		DmEnrollmentSvc	Manual	Configurado	
Servicio de inspección de red de Windows Defender		WdNisSvc	Manual	Configurado	
Servicio de instalación de dispositivos		DeviceInstall	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V		vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V		vmicheartbeat	Manual	Configurado	
Servicio de licencia de cliente (ClipSVC)		ClipSVC	Manual	Configurado	
Servicio de lista de redes		netprofm	Manual	Configurado	
Servicio de notificación de eventos de sistema		SENS	Automático	Configurado	
Servicio de Panel de escritura a mano y teclado táctil		TabletInputService	Deshabilitado	Configurado	
Servicio de perfil de usuario		ProfSvc	Automático	Configurado	
Servicio de plataforma de dispositivos conectados		CDPSvc	Automático	Configurado	
Servicio de protocolo de túnel de sockets seguros		SstpSvc	Manual	Configurado	
Servicio de puerta de enlace de nivel de aplicación		ALG	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de registro de acceso de usuarios		UALSVC	Automático	Configurado	
Servicio de repositorio de estado		StateRepository	Manual	Configurado	
Servicio de sensores		SensorService	Manual	Configurado	
Servicio de servidor proxy KDC (KPS)		KPSSVC	Manual	Configurado	
Servicio de sincronización de hora		vmictimesync	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
de Hyper-V					
Servicio de supervisión de licencias de Windows		WLMS	Automático	Configurado	
Servicio de supervisión de sensores		SensrSvc	Manual	Configurado	
Servicio de transferencia inteligente en segundo plano (BITS)		BITS	Manual	Configurado	
Servicio de uso compartido de datos		DsSvc	Manual	Configurado	
Servicio de uso compartido de puertos Net.Tcp		NetTcpPortSharing	Deshabilitado	Configurado	
Servicio de usuario de notificaciones de inserción de Windows		WpnUserService	Manual	Configurado	
Servicio de virtualización de Escritorio remoto de Hyper-V		vmicrdv	Manual	Configurado	
Servicio de virtualización de la experiencia de usuario		UevAgentService	Deshabilitado	Configurado	
Servicio de Windows Defender		WinDefend	Automático	Configurado	
Servicio de Windows Insider		wisvc	Manual	Configurado	
Servicio de zona con cobertura inalámbrica móvil de Windows		icssvc	Deshabilitado	Configurado	
Servicio del iniciador iSCSI de Microsoft		MSiSCSI	Manual	Configurado	
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio del sistema de notificaciones de inserción de Windows		WpnService	Automático	Configurado	
Servicio enumerador de dispositivos portátiles		WPDBusEnum	Manual	Configurado	
Servicio FrameServer de la Cámara de Windows		FrameServer	Manual	Configurado	
Servicio host de		WEPHOSTSVC	Manual	Configurado	

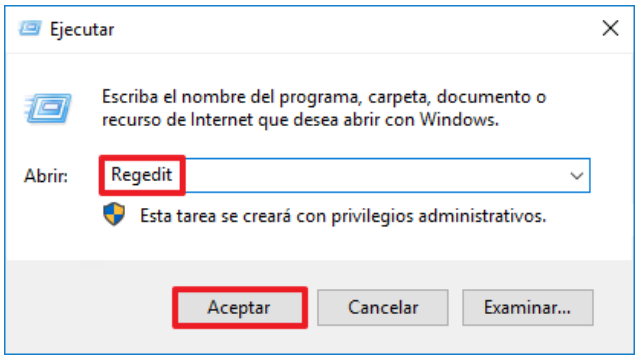
Comprobación	OK/NOK	Cómo hacerlo		
proveedor de cifrado de Windows				
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado	
Servicio Interfaz de almacenamiento en red	nsi	Automático	Configurado	
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado	
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standardcollector.service	Manual	Configurado	
Servicio telefónico	PhoneSvc	Manual	Configurado	
Servicios de cifrado	CryptSvc	Automático	Configurado	
Servicios de Escritorio remoto	TermService	Manual	Configurado	
Servidor	LanmanServer	Automático	Configurado	
Servidor del modelo de datos del mosaico	tiledatamodelsvc	Automático	Configurado	
Sincronizar host	OneSyncSvc	Automático	Configurado	
Sistema de cifrado de archivos (EFS)	EFS	Manual	Configurado	
Sistema de eventos COM+	EventSystem	Automático	Configurado	
SMP de Espacios de almacenamiento de Microsoft	smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado	
Superfetch	SysMain	Manual	Configurado	
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Tarjeta inteligente	SCardSvr	Deshabilitado	Configurado	
Telefonía	TapiSrv	Deshabilitado	Configurado	
Telemetría y experiencias del usuario conectado	DiagTrack	Automático	Configurado	
Temas	Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)	RpcLocator	Manual	Configurado	
WalletService	WalletService	Manual	Configurado	
Windows Driver	wudfsvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Foundation - User-mode Driver Framework					
Windows Installer		msiserver	Manual	Configurado	
Windows Search		WSearch	Deshabilitado	Configurado	
Windows Update		wuauserv	Manual	Configurado	
SMP de Espacios de almacenamiento de Microsoft		smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V		vmicvss	Manual	Configurado	
Superfetch		SysMain	Manual	Configurado	
Tarjeta inteligente		SCardSvr	Deshabilitado	Configurado	
Telefonía		TapiSrv	Deshabilitado	Configurado	
Telemetría y experiencias del usuario conectado		DiagTrack	Automático	Configurado	
Temas		Themes	Deshabilitado	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)		RpcLocator	Manual	Configurado	
WalletService		WalletService	Manual	Configurado	
Windows Driver Foundation - User-mode Driver Framework		wudfsvc	Manual	Configurado	
Windows Installer		msiserver	Manual	Configurado	
26. Verifique que se han asignado los permisos correctos en el sistema de archivos		Utilizando el Explorador de Windows: **"Windows+R → Explorer"** En caso de no saber dónde apunta cada una de las rutas abreviadas que se especifica, ejecute Explorer <<ruta>> donde <<ruta>> se sustituirá por la ruta abreviada. **Nota:** Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, marcándolo con el botón derecho y eligiendo la opción "Propiedades" del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá situarse en la pestaña "Seguridad". En la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios. Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados.			

Comprobación	OK/NOK	Cómo hacerlo

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\Registration	Administrador	Control total	
	System	Control total	
	Usuario	Leer y ejecutar	
%SystemRoot%\repair	Administrador	Control total	
	System	Control total	
%SystemRoot%\security	Administrador	Control total	
	System	Control total	
SystemRoot%\system32\cacls.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\clip.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\ras	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\rasadhlp.dll	Administrador	Control total	
%SystemRoot%\system32\rasauto.dll	Administrador	Control total	
%SystemRoot%\system32\rasautou.exe	Administrador	Control total	
%SystemRoot%\system32\raschap.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrnm.h	Administrador	Control total	
%SystemRoot%\system32\rasctrs.dll	Administrador	Control total	
%SystemRoot%\system32\rasctrs.ini	Administrador	Control total	
%SystemRoot%\system32\rasdial.exe	Administrador	Control total	
%SystemRoot%\system32\rasmans.dll	Administrador	Control total	
%SystemRoot%\system32\rasmontr.dll	Administrador	Control total	
%SystemRoot%\system32\rasphone.exe	Administrador	Control total	
%SystemRoot%\system32\rasppp.dll	Administrador	Control total	
%SystemRoot%\system32\rastapi.dll	Administrador	Control total	

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\system32\rastls.dll	Administrador	Control total	
%SystemRoot%\system32\runonce.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\secedit.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\telnet.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tftp.exe	Administrador	Control total	
	System	Control total	
%SystemRoot%\system32\tracert.exe	Administrador	Control total	
	System	Control total	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>27. Verifique los valores del registro.</td><td></td><td>Compruebe los valores del registro definidos en los Controladores de Dominio que pertenezcan al grupo categorizado como categoría alta siguiendo los criterios del ENS, mediante el uso del “Editor del Registro”.
“Windows+R → Regedit”
El Control de cuentas de usuario solicitará elevación de privilegios. Pulse “Sí” para continuar.
 

<table>
<tr><th>Valor del registro</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod</td><td>0</td><td></td></tr>
<tr><td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun</td><td>255</td><td></td></tr>
<tr><td>HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation</td><td>1</td><td></td></tr>
<tr><td>HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode</td><td>1</td><td></td></tr>
<tr><td>HKLM\System\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta</td><td>10</td><td></td></tr>
<tr><td>HKLM\System\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog</td><td>1</td><td></td></tr>
<tr><td>HKLM\System\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog</td><td>20000</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Valor del registro	Valor	OK/NOK
		HKLM\System\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog	20	
		HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel	90	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect	0	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime	300000	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery	0	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect	1	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions	2	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions	3	
		HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TCPMaxPortsExhausted	5	

ANEXO A.5. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD

ANEXO A.5.1. IMPLEMENTACIÓN DE CORTAFUEGOS CON SEGURIDAD AVANZADA

El presente Anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación del cortafuegos con seguridad avanzada con objeto de ofrecer mecanismos de protección adicionales a los servidores Windows Server 2016. Este anexo ha sido diseñado para atender al principio de mínima exposición que faculta a un sistema a reducir los riesgos, minimizando los puntos de entrada al mismo.

Debe tenerse en consideración que la implementación de un firewall de servidor dependerá, en sí misma, de la funcionalidad del mismo y de los servicios que éste ofrece a la infraestructura. No se tendrá, evidentemente, la misma funcionalidad y, por lo tanto, la necesidad de puertos abiertos, en un servidor que actúe como Controlador de Dominio que en otro que funcione como servidor de ficheros exclusivamente. A partir de Windows Vista, Microsoft proporciona un servicio de cortafuegos con seguridad avanzada. Éste permite realizar el control para las diferentes categorías de redes en la que puede estar un sistema: pública, privada o dominio.

De forma predeterminada, el control de la configuración del Firewall de Windows con Seguridad Avanzada se establece a nivel local. No obstante, existe la posibilidad de realizar un control centralizado a través de la aplicación de objetos de políticas de grupo. Esta opción proporciona dos condiciones fundamentales:

a) Mejorar las condiciones de seguridad, al establecer las mismas por parte de los administradores de dominio, sin que una alteración de tipo local afecte a dicha configuración.

b) Centralizar la administración, de tal forma que exista un único punto de control.

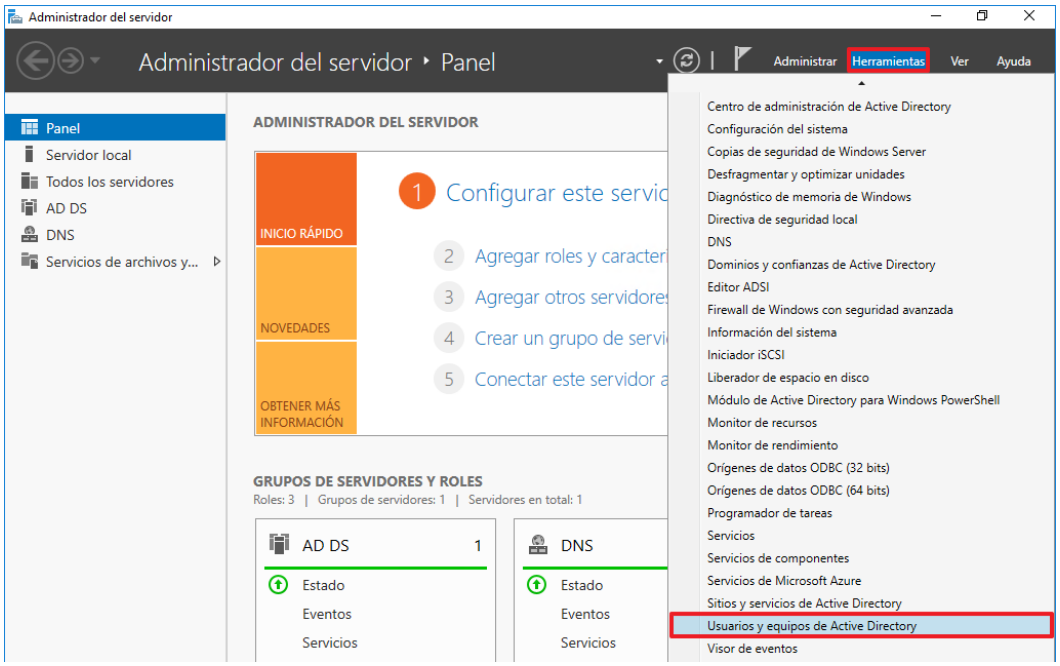
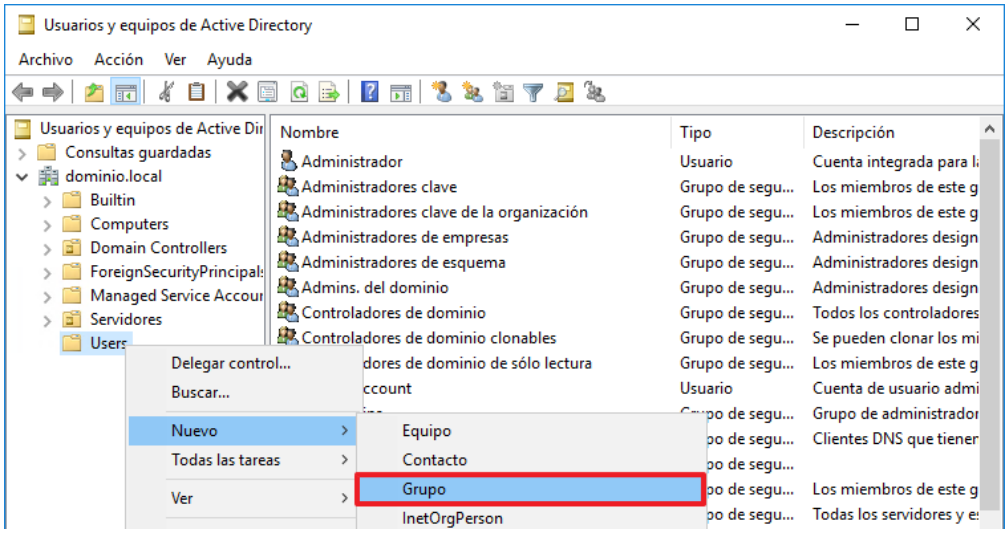
No obstante, este mecanismo de administración centralizada exige, por parte de los administradores, un control elevado y tener claras la creación y aplicación de diferentes políticas de seguridad, en función de las necesidades demandadas por los servicios.

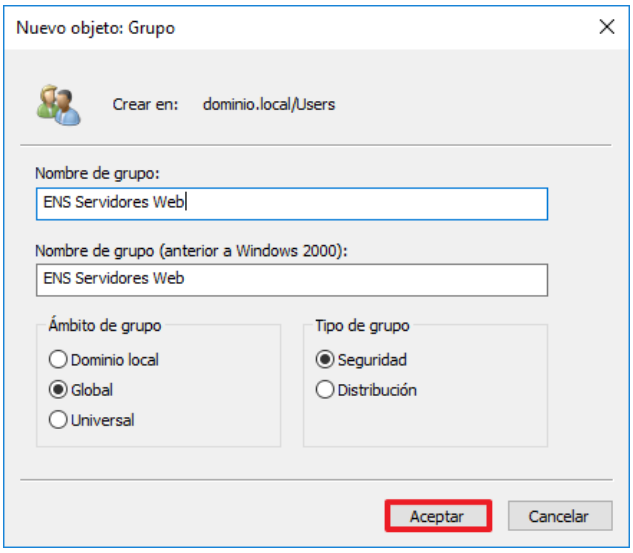
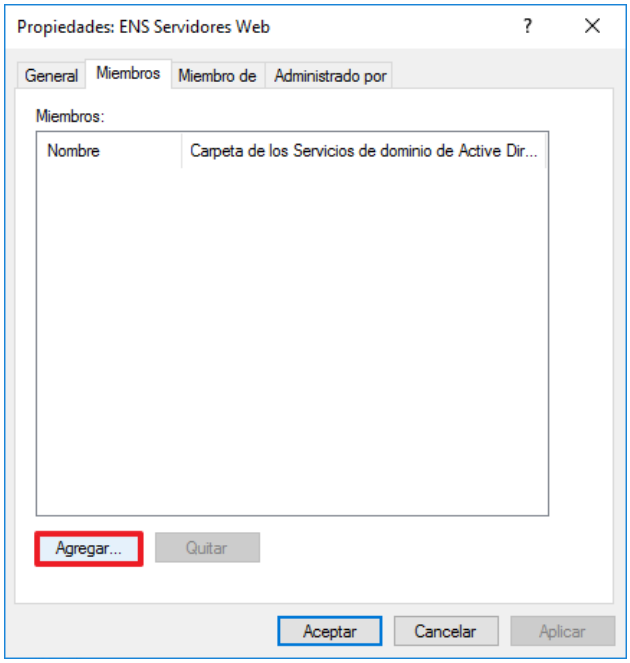
En este anexo, se darán una serie de recomendaciones necesarias para la creación y gestión de GPO para la administración centralizada de la seguridad del cortafuegos. Como en los anexos previos, los operadores deberán realizar pruebas en entornos de preproducción antes de realizar una implementación en el entorno de producción.

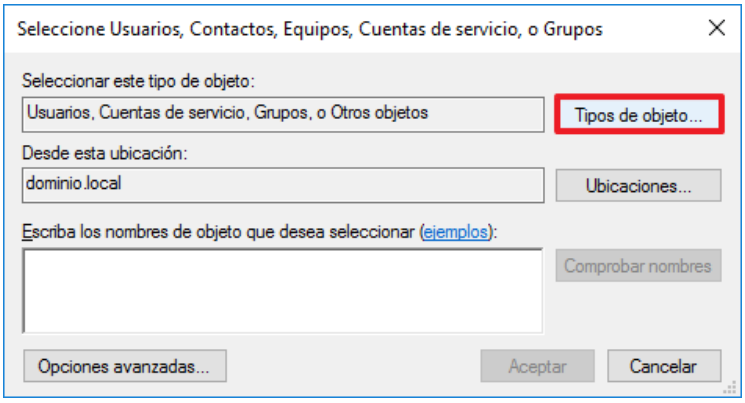
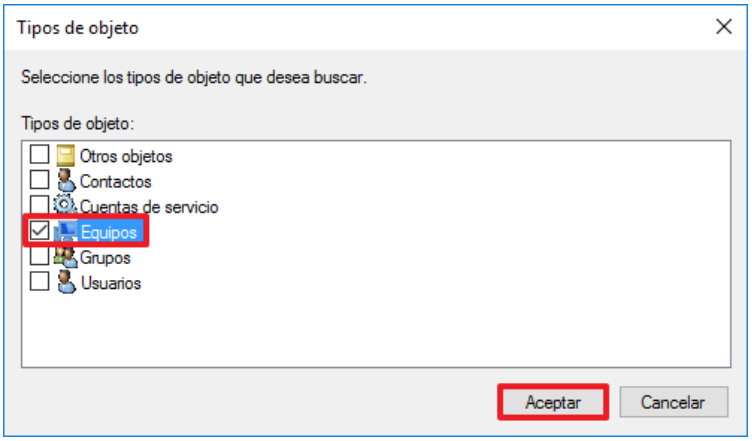
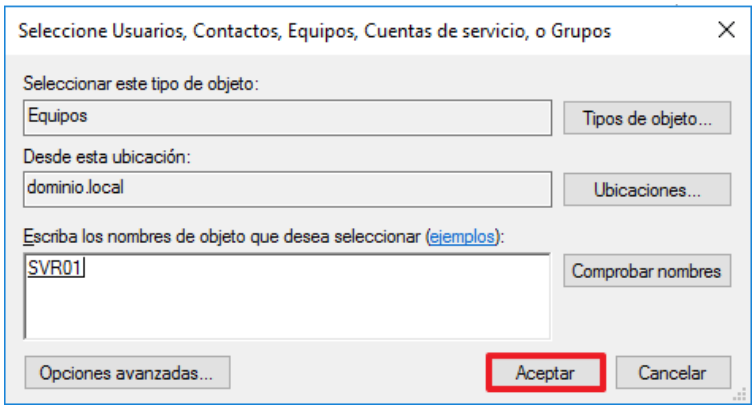
1. CREACIÓN DE GRUPOS PARA LA ASIGNACIÓN DE OBJETOS DE POLÍTICA DE GRUPO

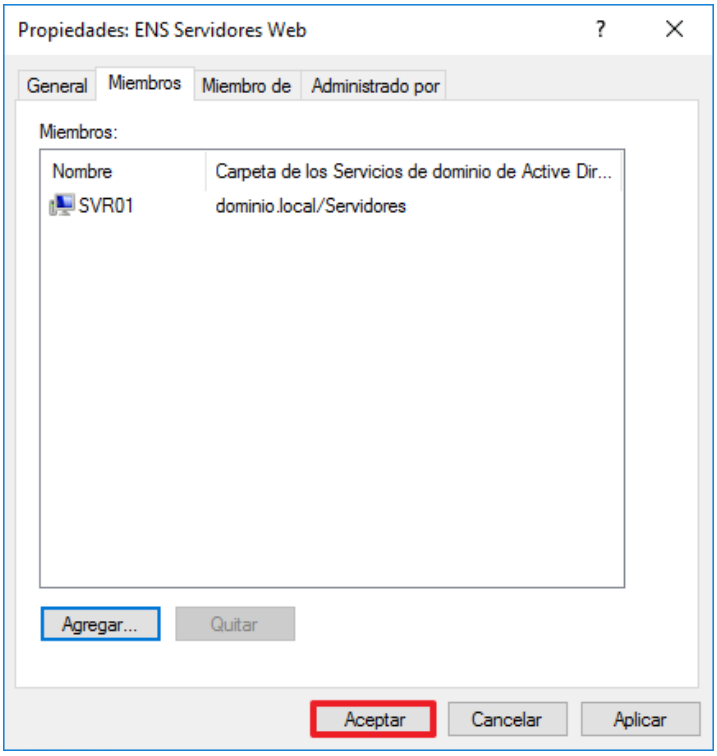
Motivado por el hecho de las diferentes configuraciones aplicables a los diferentes servidores de una organización y en base a su funcionalidad, podrán aplicarse diferentes objetos GPO filtrados por grupos de equipos. Para realizar dicho filtrado, será necesaria la creación, de forma previa, de los grupos de equipos necesarios en el Directorio Activo. En este sentido, se considera conveniente agrupar los servidores en base a los servicios y puertos que necesiten tener abiertos.

Nota: En el presente ejemplo se va a crear una política de grupo para la aplicación de política de cortafuegos para un conjunto de servidores web que sirven aplicaciones web por puerto 80 y 443.

Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Inicie la herramienta de usuarios y equipos del Directorio Activo. Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Usuarios y equipos de Active Directory"** 
4.	Despliegue el dominio y vaya a la carpeta donde se encuentran sus servidores o bien donde desee mantener dichos grupos. En el ejemplo se empleará la carpeta "Users".
5.	Pulse con el botón derecho sobre dicha carpeta y seleccione la opción **"Nuevo → Grupo".** 

Paso	Descripción
6.	Introduzca como nombre “ENS Servidores Web”. Deje el resto de opciones como está y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar los GPO para la aplicación de seguridad en el cortafuegos.  **Nota:** Recuerde que este paso a paso es un ejemplo de cómo configurar un objeto de política de grupo para aplicar sobre un conjunto de servidores determinados con motivo de aplicarles una configuración determinada. En el presente ejemplo se basa en la agrupación de servidores web.
7.	Abra el nuevo grupo creado haciendo doble clic sobre él y vaya a la pestaña “Miembros”.
8.	Pulse el botón “Agregar…”. 

Paso	Descripción
9.	Pulse el botón de “Tipos de objeto…”. 
10.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 
11.	Introduzca el nombre de los servidores o utilice las opciones avanzadas para agregar todos aquellos servidores miembro que cumplan las condiciones de aplicación del GPO para la configuración del firewall. En este caso, servidores que proporcionan aplicaciones Web por los puertos 80 y 443.
12.	Pulse el botón “Aceptar” para agregar la selección. 

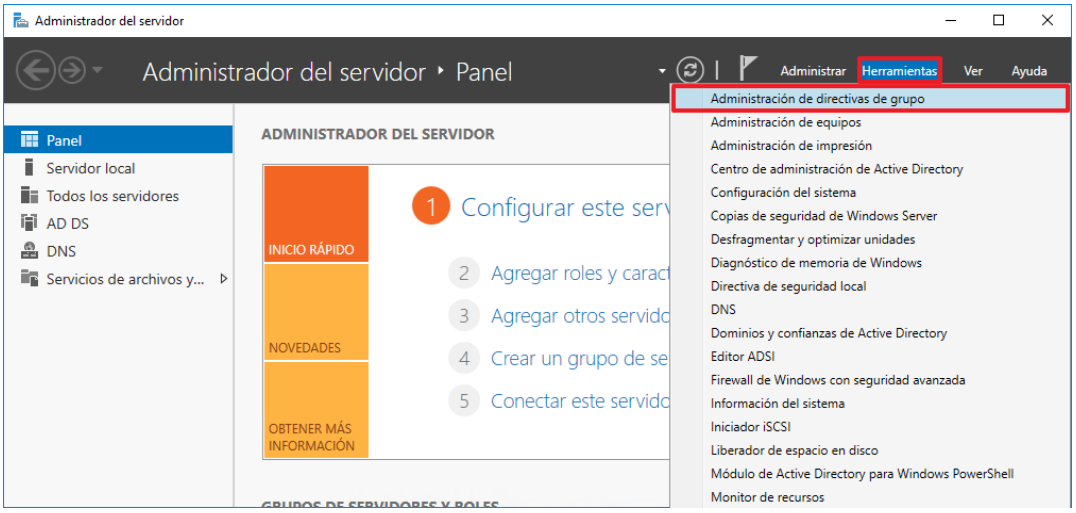
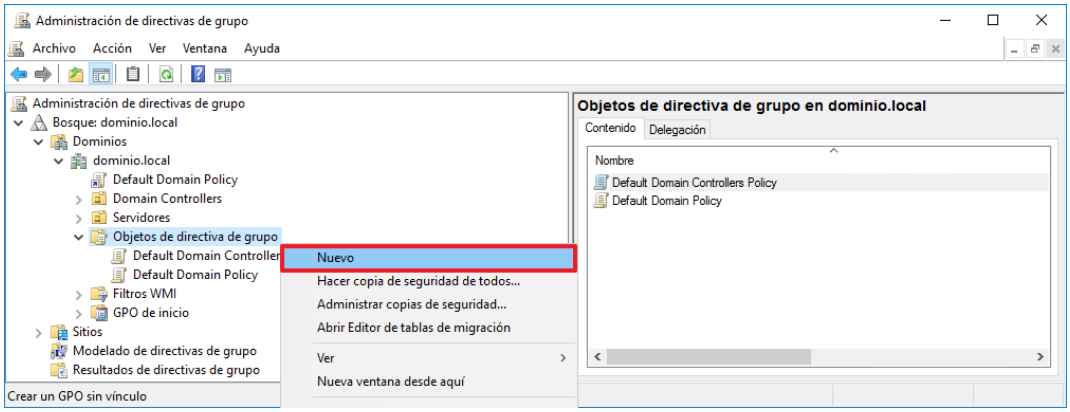
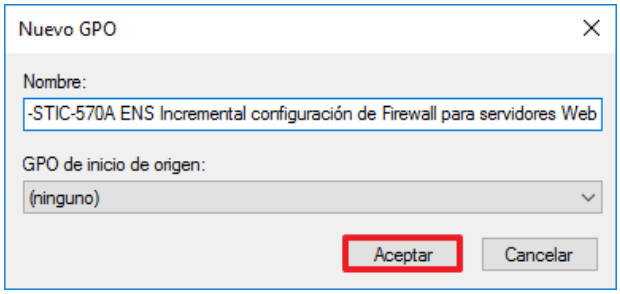
Paso	Descripción
13.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo. 
14.	Cierre la herramienta “Usuarios y equipos de Directorio Activo”. **Nota:** El grupo creado, aunque en el ejemplo se va a emplear para la configuración del cortafuegos, se podría utilizar para la aplicación de una configuración de seguridad aplicable a través de GPO diferentes del resto de servidores de la organización.

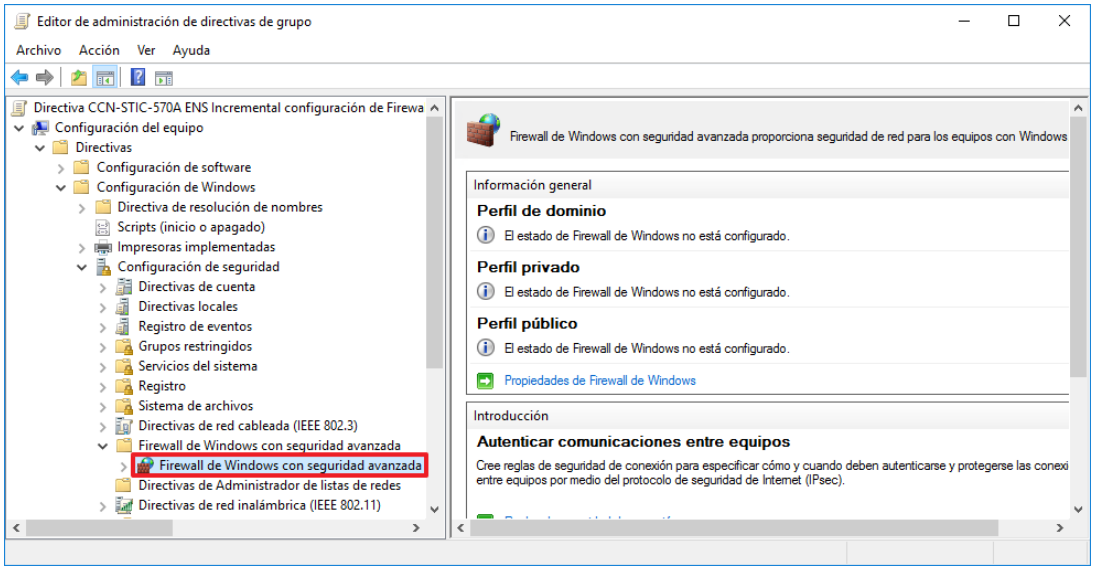
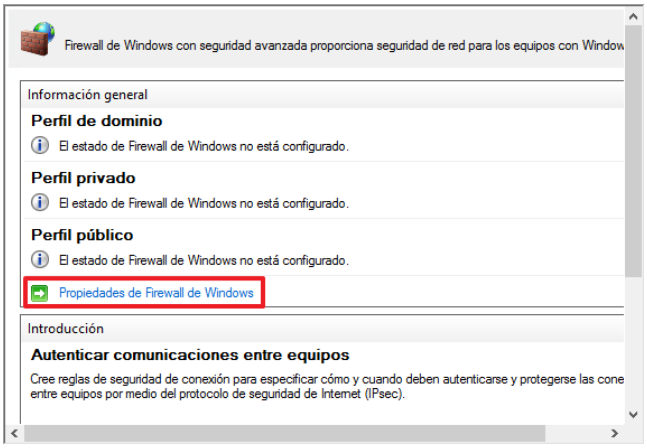
2. CREACIÓN Y ASIGNACIÓN DE LOS OBJETOS GPO PARA LA APLICACIÓN DE UNA POLÍTICA DE CORTAFUEGOS

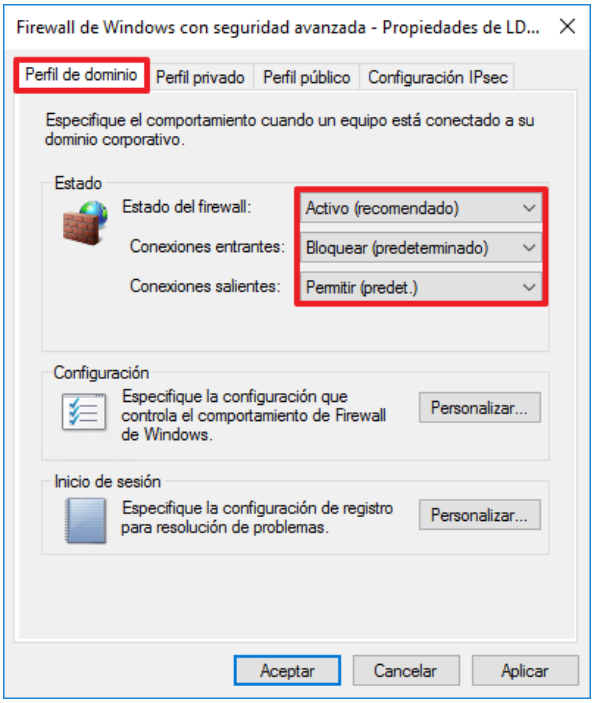
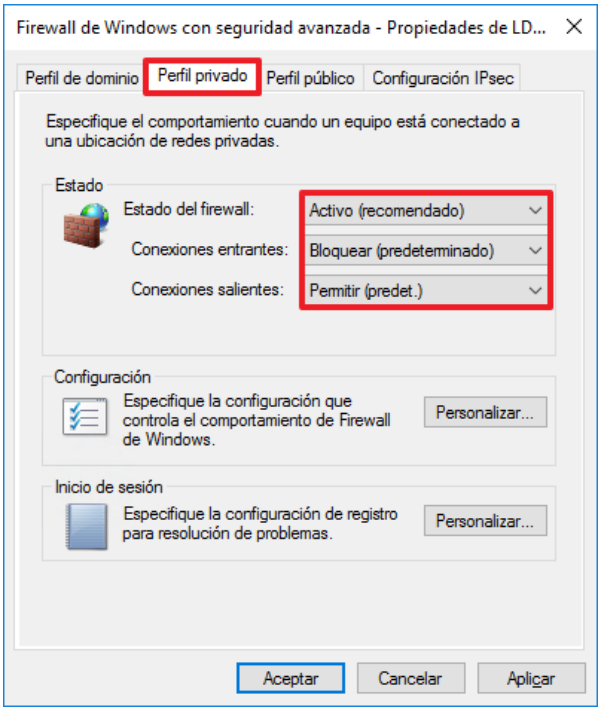
Una vez creado el grupo correspondiente, se procederá a crear y asignar la política de cortafuegos. Deberá tomar en consideración las necesidades de qué puertos y/o aplicaciones o servicios es necesario permitir para el conjunto de servidores.

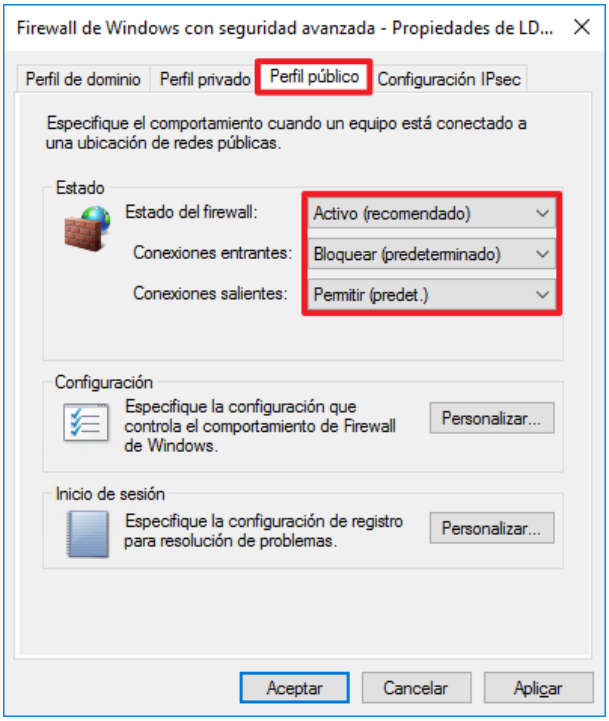
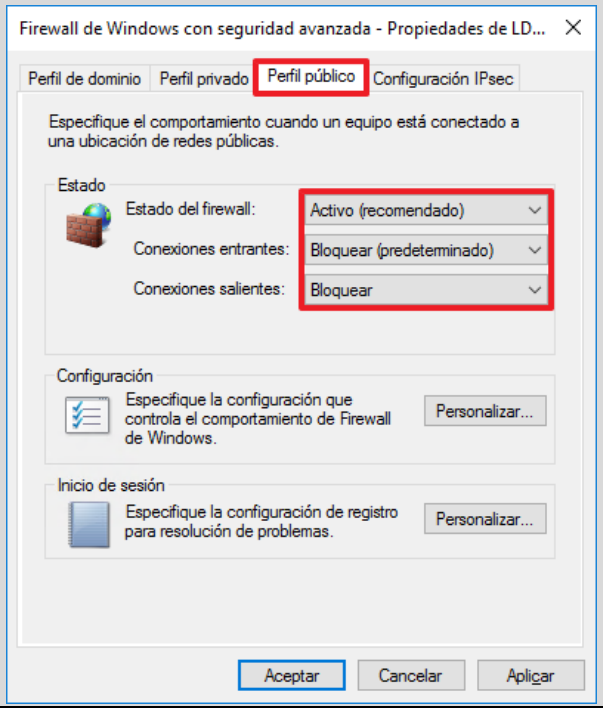
Nota: En el presente ejemplo, se va a crear una política de grupo para la aplicación de política de cortafuegos para un conjunto de servidores web que sirven aplicaciones Web por puerto 80 y 443.

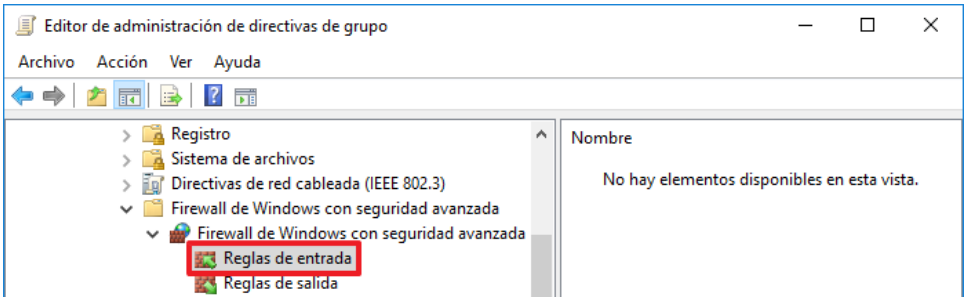
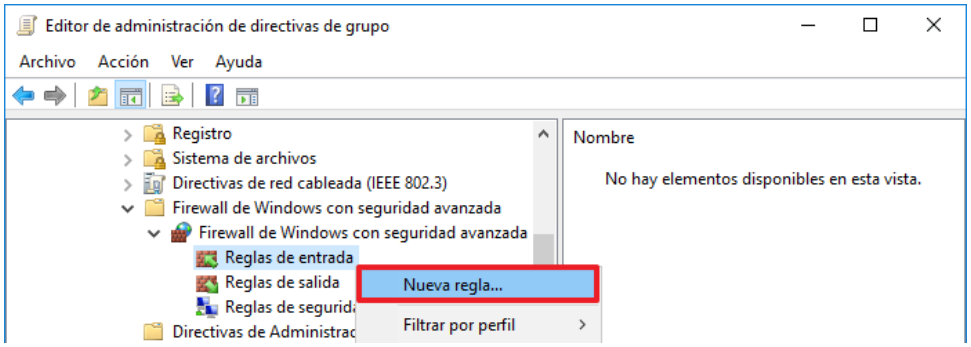
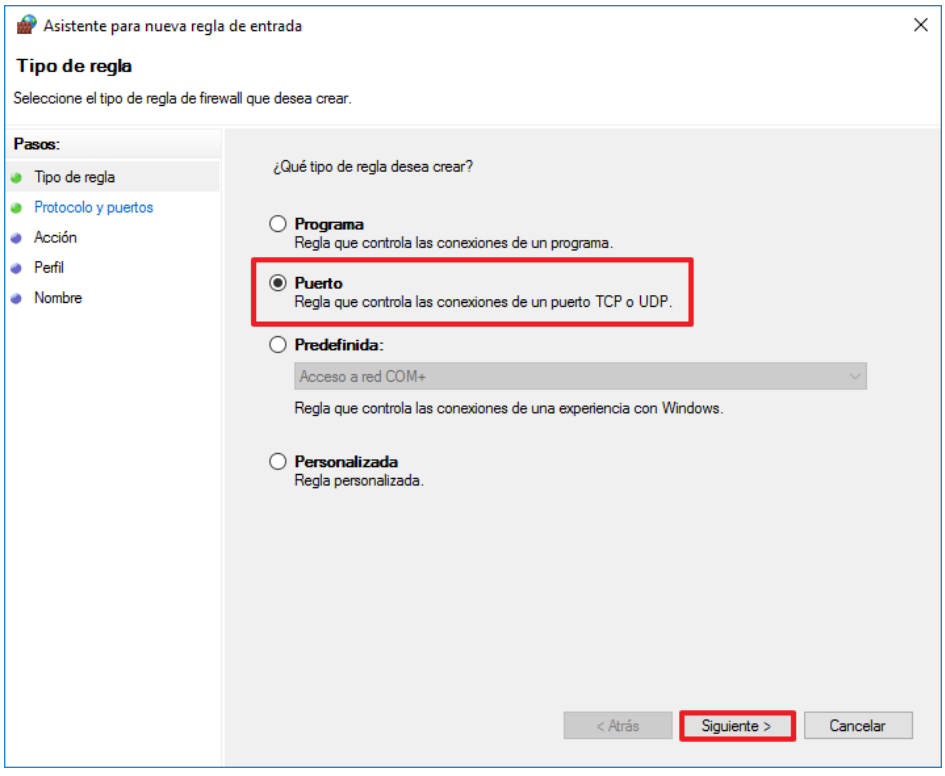
Paso	Descripción
15.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.
16.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

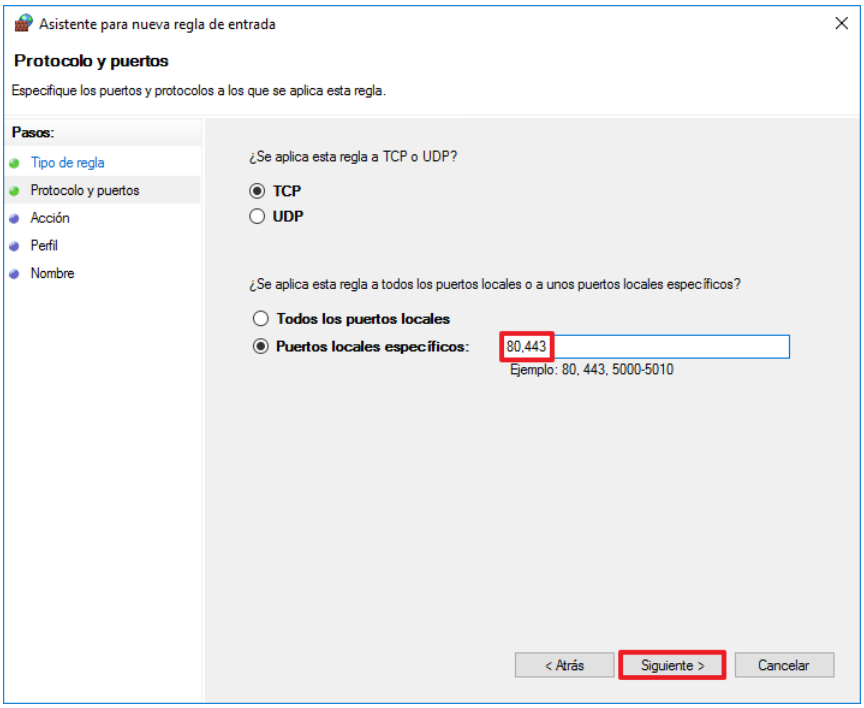
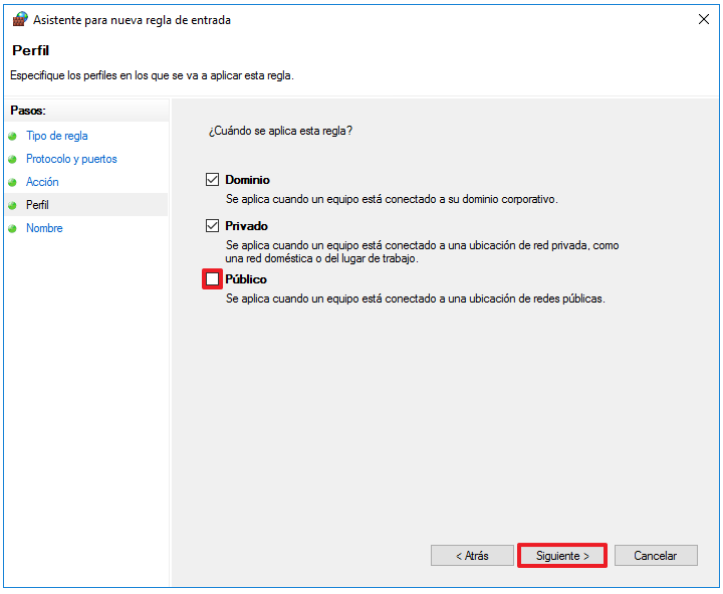
Paso	Descripción
17.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”** 
18.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”.
19.	Pulse con el botón derecho, sobre dicha y carpeta y seleccione la opción “Nuevo”. 
20.	Introduzca como nombre “CCN-STIC-570A ENS Incremental configuración de Firewall para servidores Web” y pulse el botón “Aceptar”. 
21.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”.

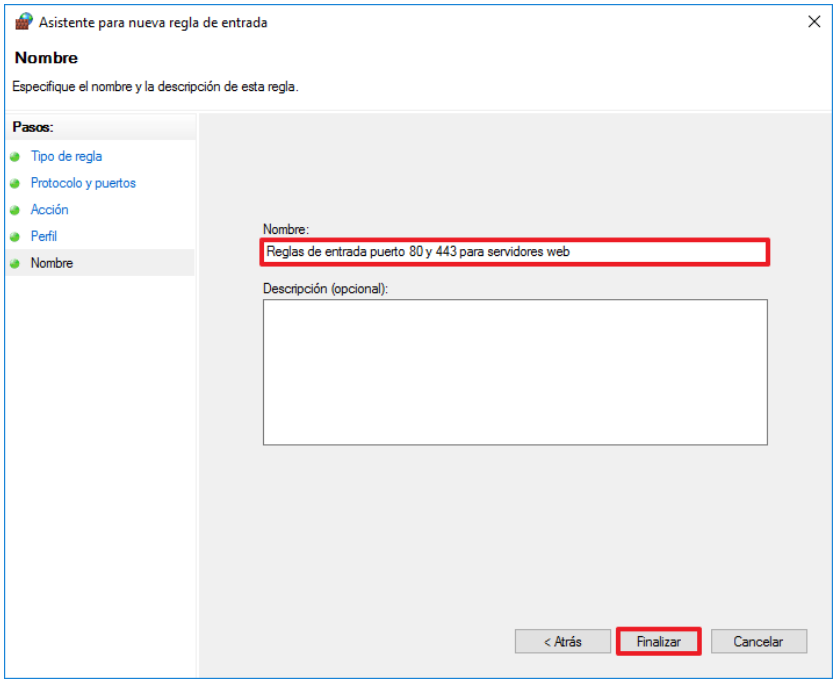
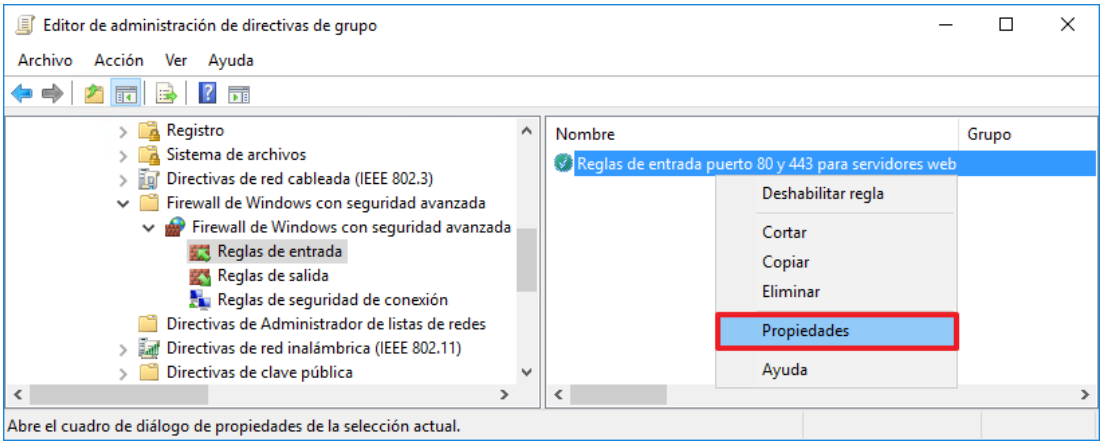
Paso	Descripción
22.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Firewall de Windows con seguridad avanzada → Firewall de Windows con seguridad avanzada – LDAP://CN=..."** 
23.	Pulse sobre las "Propiedades de Firewall de Windows" que aparecen en la configuración de "Información General", existentes en el panel derecho. 

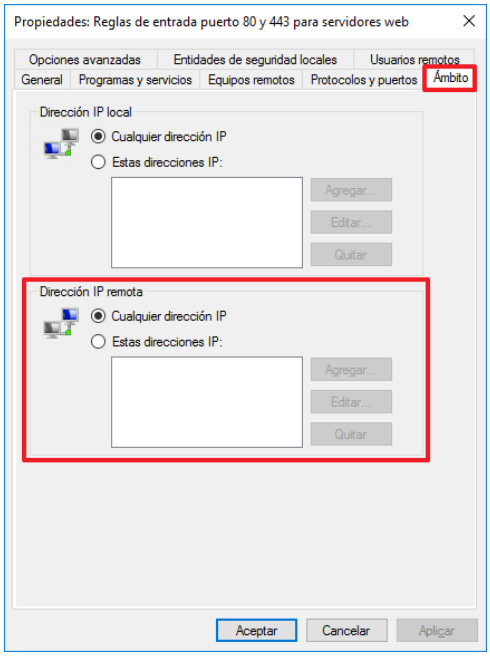
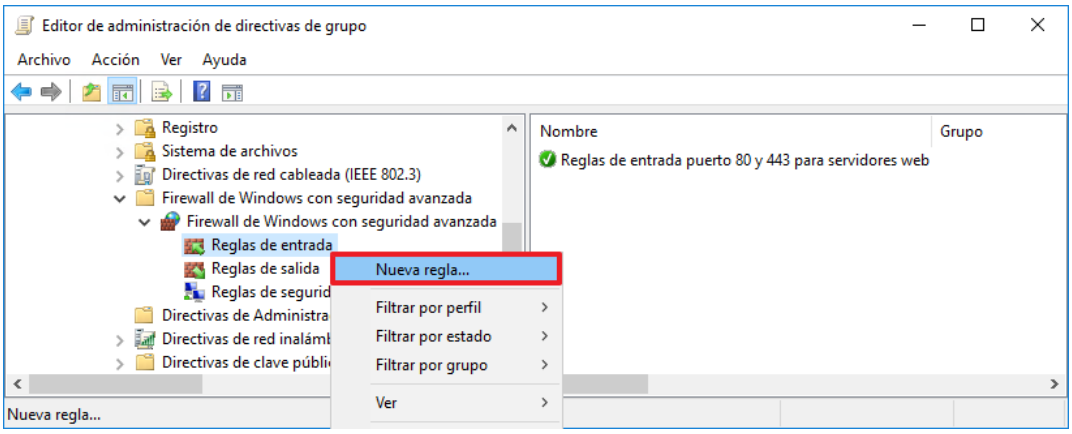
Paso	Descripción
24.	La primera de las pestañas “Perfil de dominio” configúrela como aparece en la siguiente imagen: 
25.	A continuación, vaya a la pestaña “Perfil privado” y configúrela tal y como aparece en la siguiente imagen: 

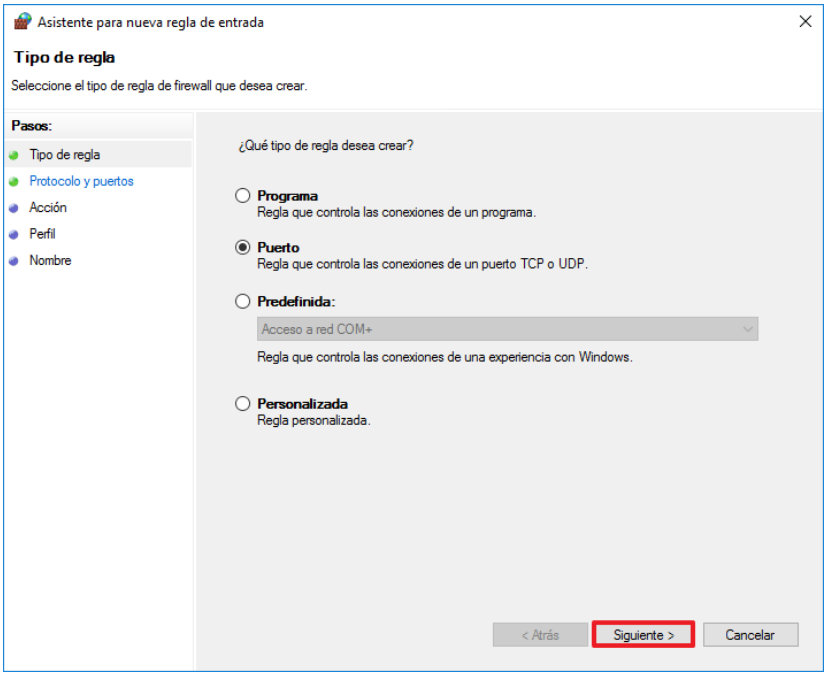
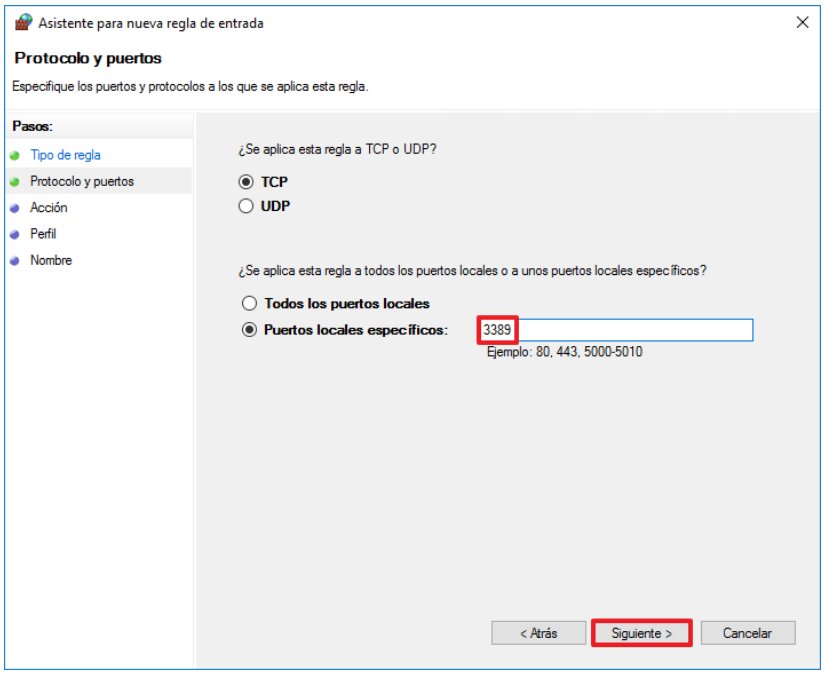
Paso	Descripción
26.	Vaya posteriormente a la pestaña “Perfil público” y establezca la configuración que aparece en la siguiente imagen:  **Nota:** En el caso de que los servidores proporcionaran servicios de categoría alta, sería recomendable que el perfil público quedara configurado como aparece en la siguiente imagen. 
27.	Pulse el botón “Aceptar” para guardar los cambios introducidos en los diferentes perfiles.

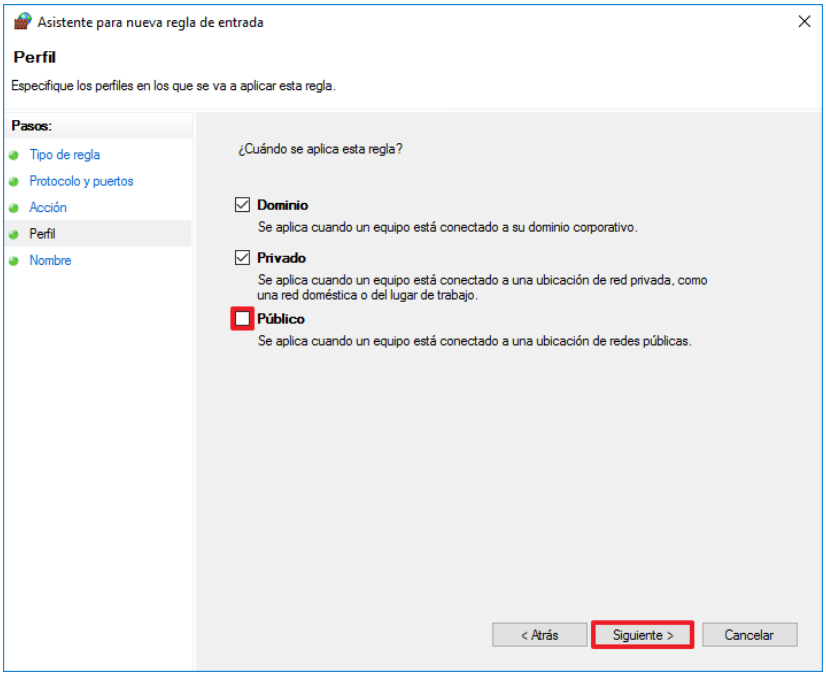
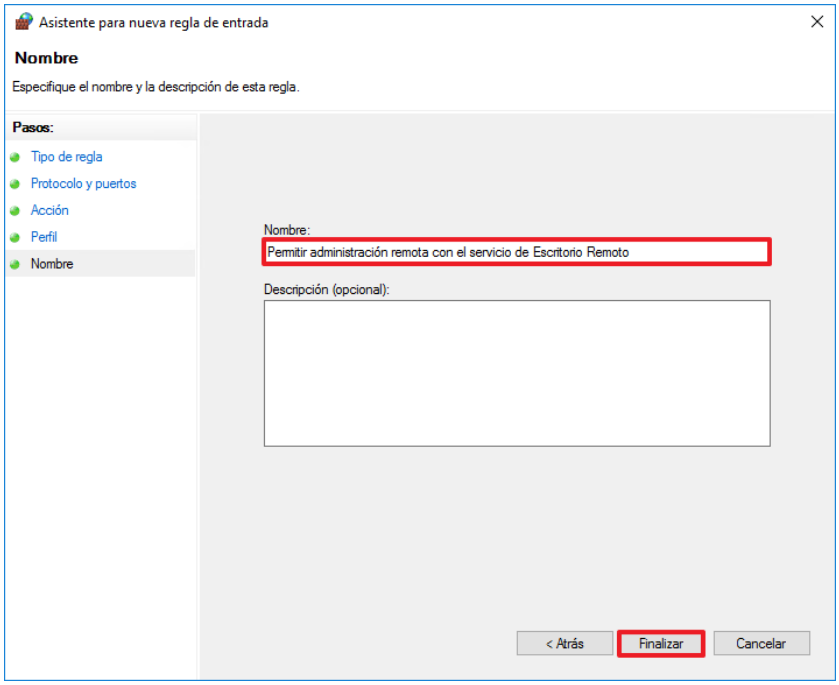
Paso	Descripción
28.	Despliegue el Firewall con seguridad avanzada y vaya a “Reglas de entrada”. 
29.	Pulse con el botón derecho sobre “Reglas de entrada” y seleccione la opción “Nueva regla…”. 
30.	En el inicio del asistente seleccione la opción de “Puerto” y pulse el botón “Siguiente >”. 

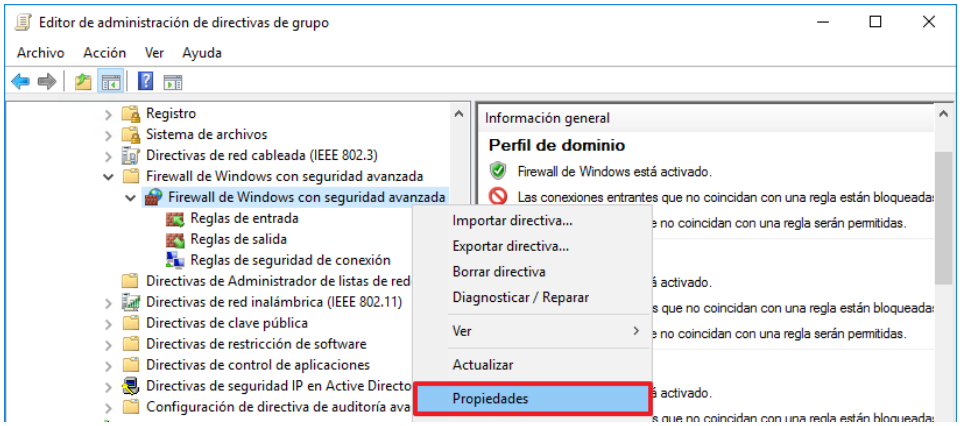
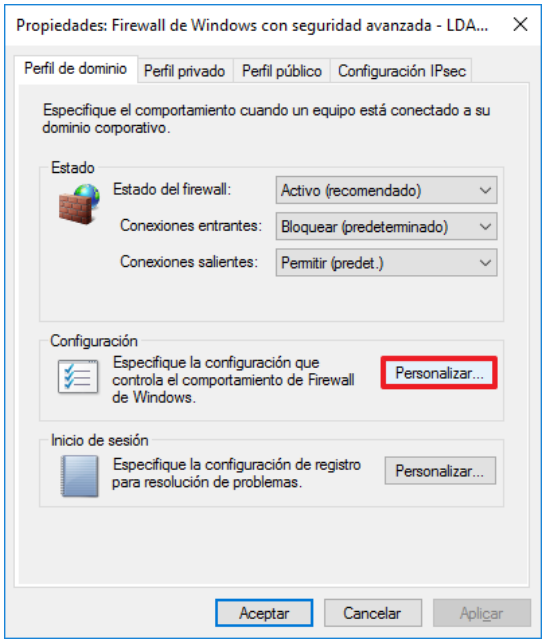
Paso	Descripción
31.	En la opción de “Puertos locales específicos” introduzca “80, 443”. Si los servidores web escucharan peticiones por otros puertos, debería introducir también dichos puertos. Pulse el botón “Siguiente >”. 
32.	En la pantalla de “Acción”, mantenga la configuración y pulse el botón “Siguiente >”.
33.	En “Perfil”, deje marcados los perfiles “Dominio” y “Privado” y desmarque el perfil “Público”. Pulse el botón “Siguiente >”. 

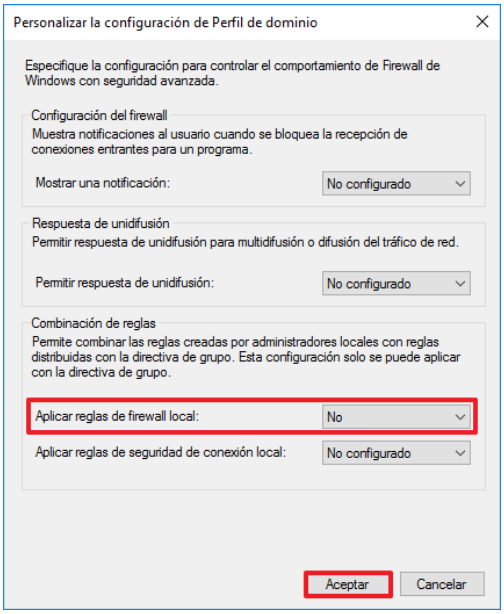
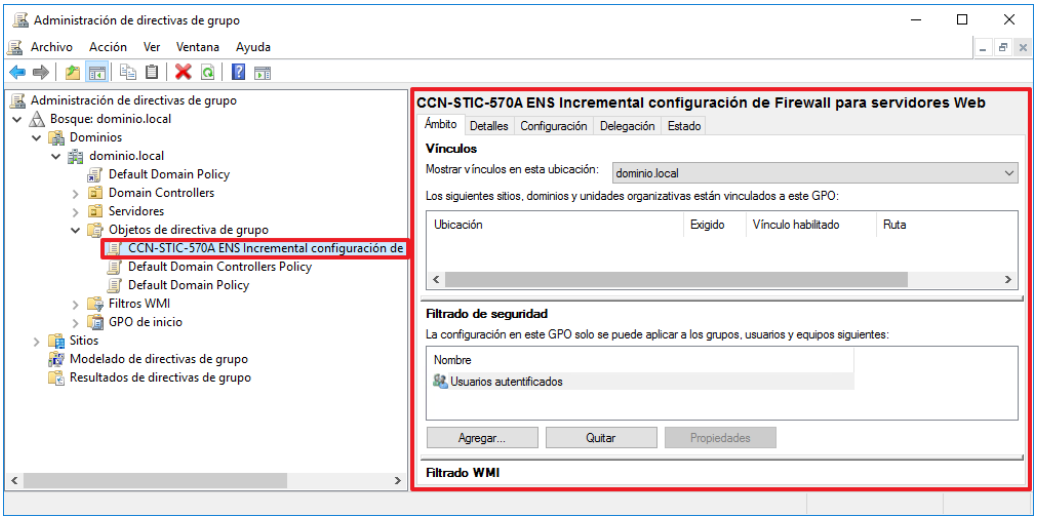
Paso	Descripción
34.	Asigne un nombre a la nueva regla de entrada que está creando y pulse el botón “Finalizar”. 
35.	La nueva regla ya se encuentra creada. Puede editarla pulsando con el botón derecho del ratón sobre la misma y seleccionando la opción “Propiedades”. 

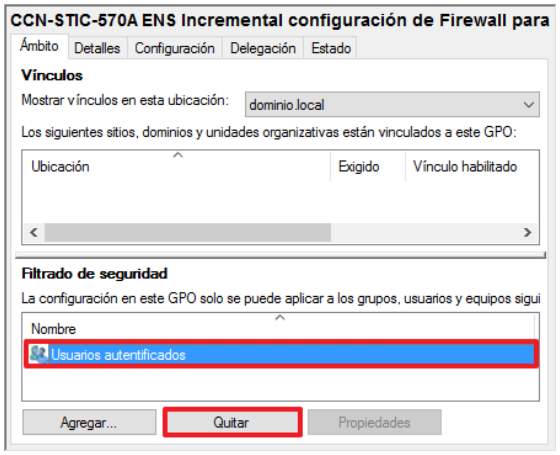
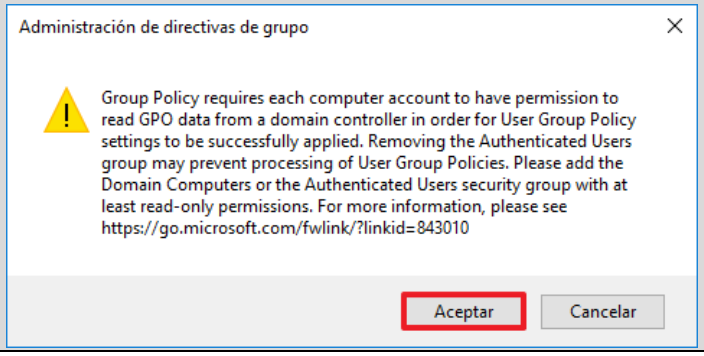
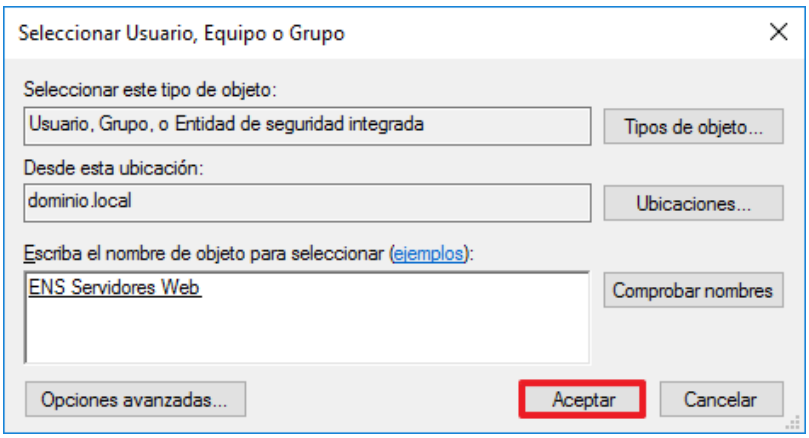
Paso	Descripción
36.	Podrían, por ejemplo, limitarse las IP remotas o rangos de redes que podrían conectarse a los servidores a través de los puertos 80 y 443. De forma predeterminada, se admite cualquier IP, pero podría establecerse un límite a las mismas mediante la pestaña “Ámbito”. 
37.	Una vez creadas las reglas de entrada para los puertos de los servicios web, debería determinarse si existe la necesidad de abrir otros puertos, por ejemplo, para realizar administración remota a través del servicio de escritorio remoto de Windows. En este caso, se determina además la necesidad para estos servidores de hacer administración remota con el protocolo RDP a través del puerto 3389.
38.	Pulse nuevamente con el botón derecho sobre “Reglas de entrada” y seleccione la opción “Nueva regla…”. 

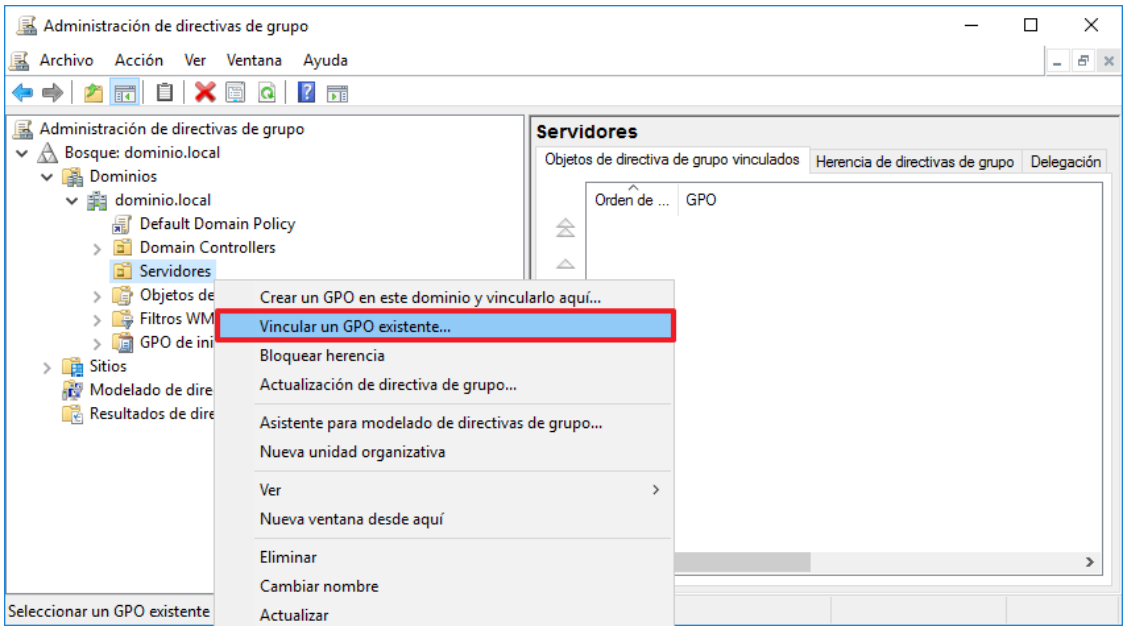
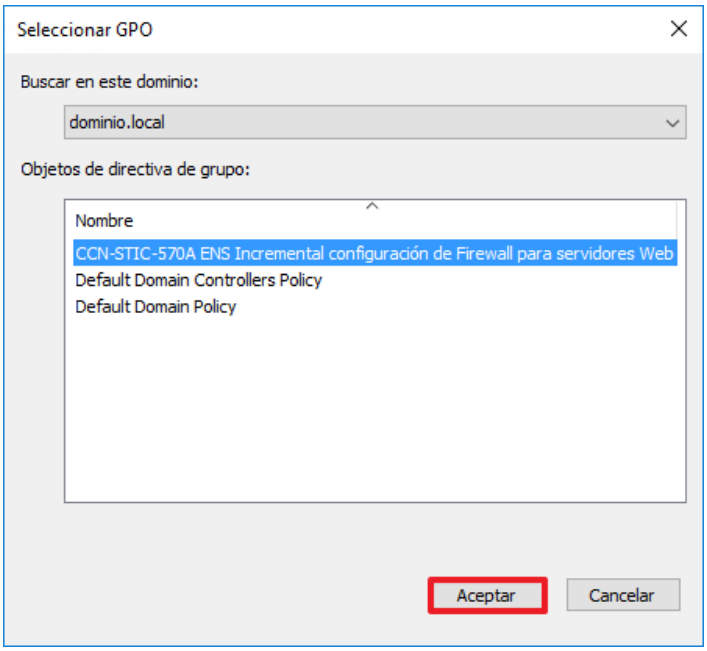
Paso	Descripción
39.	En el inicio del asistente seleccione la opción de “Puerto” y pulse el botón “Siguiente >”. 
40.	En la opción de “Puertos locales específicos” introduzca “3389” y pulse el botón “Siguiente >”. 
41.	En la pantalla de acción, mantenga la configuración y pulse el botón “Siguiente >”.

Paso	Descripción
42.	En “perfil”, deje marcados los perfiles “Dominio” y “Privado” y desmarque el perfil “público”. Pulse el botón “Siguiente >”. 
43.	Asigne un nombre a la nueva regla de entrada que está creando y pulse el botón “Finalizar”. 
44.	Como en el caso previo, debería limitarse el rango de direcciones IP que podrían realizar conexión remota para la administración por RDP. Establezca la configuración como se mostró en el paso 31.

Paso	Descripción
45.	Por último, podría resultar factible que se quisiera poder realizar conexión por RPC al equipo para intercambiar ficheros con el mismo. Para ello, deberían crearse reglas para permitir conexión a los puertos 135, 137, 139 y 445 tanto de UDP como de TCP, puesto que la apertura de estos puertos podría impactar significativamente en la seguridad de los servidores debido a que tradicionalmente se han empleado para la dispersión de gusanos tales como "Conficker". Debería, por tanto, limitarse el acceso a direcciones IP determinadas, como las de los administradores y/o desarrolladores, tal y como se mostró en el paso 31.
46.	En el caso de que el servidor que se está configurando fuera de categoría básica o media, deberá cerrarse la política y continuar en el paso 53. En el caso de que la categoría del servidor fuera alta, deberá continuar con los siguientes pasos.
47.	Pulse con el botón derecho del ratón "Firewall con seguridad avanzada – LDAP://CN…" y seleccione la opción "Propiedades". 
48.	En la pestaña de dominio pulse el botón "Personalizar" del apartado configuración. 

Paso	Descripción
49.	En “Combinación de reglas”, en la opción “Aplicar reglas de firewall local” seleccione “No” y pulse el botón “Aceptar”. 
50.	Haga lo mismo para los perfiles “Privado” y “Público”.
51.	Una vez modificados los tres perfiles pulse el botón “Aceptar”. Esto impedirá que la configuración de cortafuegos que se realice localmente tenga validez. Solo será de aplicación la configuración del dominio. **Nota:** Tenga en cuenta este hecho para agregar reglas que se estuvieran aplicando, localmente en los servidores, al objeto GPO que se está creando”.
52.	Cierre la política creada.
53.	Una vez creada la política, esta deberá asignarse al grupo creado en el punto 5 del presente anexo. Para ello, seleccione la política recién creada y vaya al panel derecho de su configuración. 

Paso	Descripción
54.	Seleccione el grupo “Usuarios autentificados” y pulse el botón “Quitar”. 
55.	Cuando salga la advertencia, preguntando si desea quitar el privilegio de delegación, diga que “Sí”. **Nota:** En caso de que aparezca la siguiente advertencia ignórela y pulse “Aceptar”. 
56.	A continuación pulse el botón “Agregar”.
57.	Introduzca el nombre del grupo creado en el primer punto del presente Anexo y pulse el botón “Aceptar”. 

Paso	Descripción
58.	Únicamente queda realizar la asignación de la política. Para ello, identifique el lugar dentro del Directorio Activo donde se ubican estos servidores y asigne allí la política. Si los servidores se ubicaran en diferentes Unidades Organizativas, puede buscar un lugar común desde donde cuelguen las diferentes ubicaciones o bien asignar el GPO en cada una de las Unidades Organizativas. En el ejemplo los servidores Web se encuentran ubicados en la Unidad Organizativa “Servidores”.
59.	Seleccione la Unida Organizativa y pulsando con el botón derecho haga uso de la opción “Vincular un GPO existente…”. 
60.	En la pantalla de selección, marque el GPO creado previamente y pulse el botón “Aceptar”. 

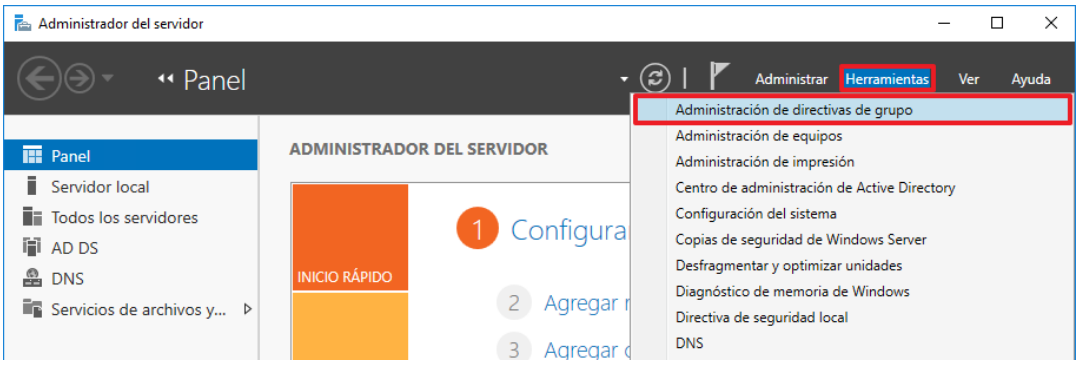
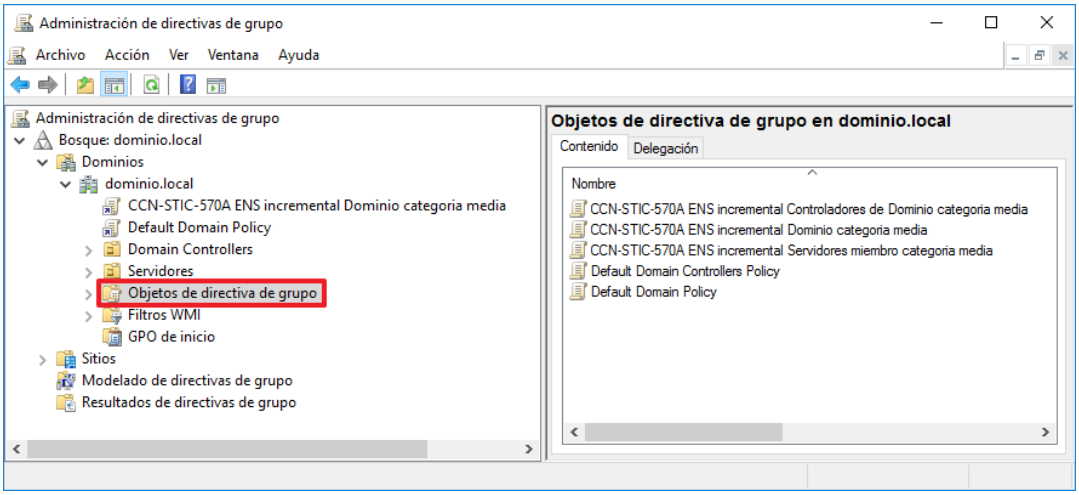
Paso	Descripción
61.	La nueva GPO ya estará creada y asignada correctamente al grupo de servidores que le corresponde.
62.	Deberá crear tantos objetos de GPO como fueran necesarios, siendo asignados a los Servidores Windows Server 2016. **Nota**: La documentación existente en la web de Technet o MSDN de Microsoft le podrá servir de orientación para conocer los puertos que emplean los servicios y aplicaciones de productos Microsoft. La siguiente URL muestra por ejemplo los puertos empleados por el Servicio de Directorio que le es de aplicación a los controladores de dominio. https://msdn.microsoft.com/en-us/library/dd772723(v=ws.10).aspx

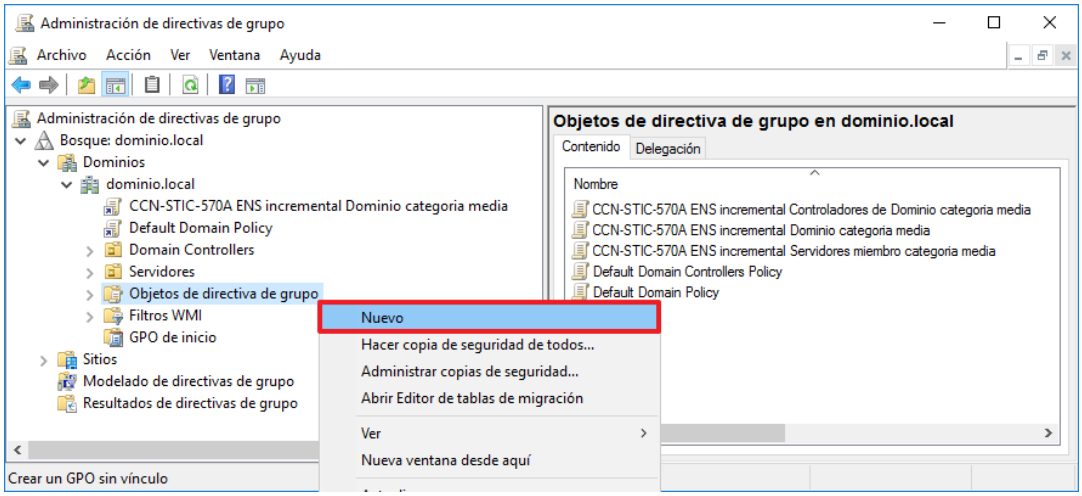
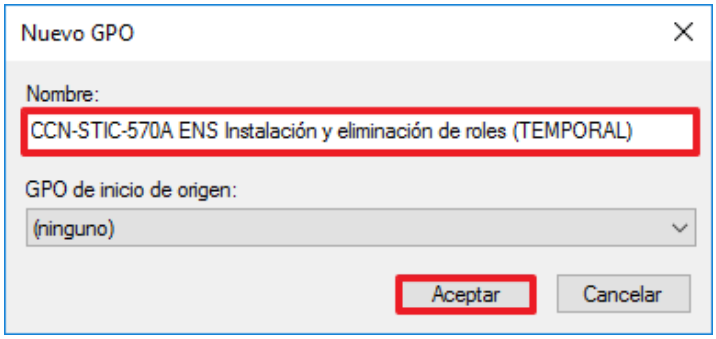
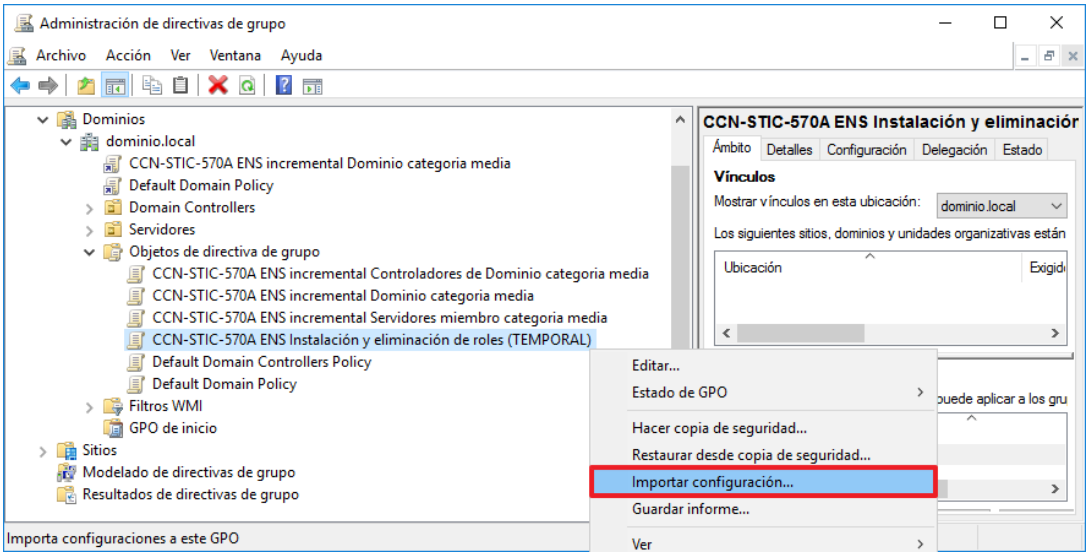
ANEXO A.5.2. INSTALACIÓN DE ROLES ADICIONALES EN SERVIDOR MIEMBRO O CONTROLADOR DE DOMINIO QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA O ALTA DEL ENS

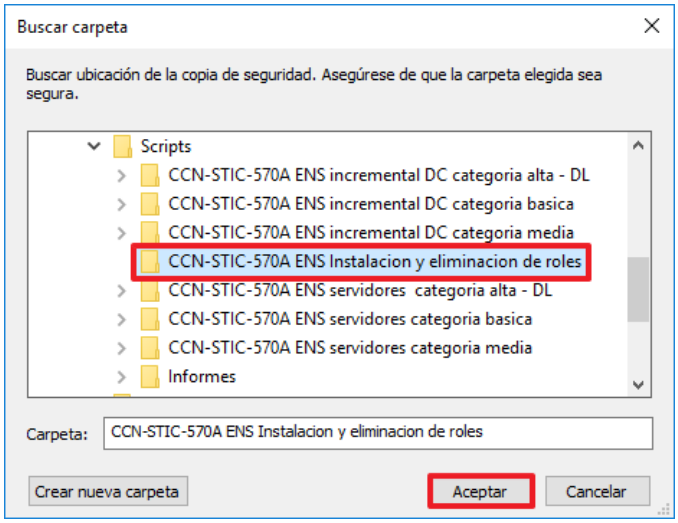
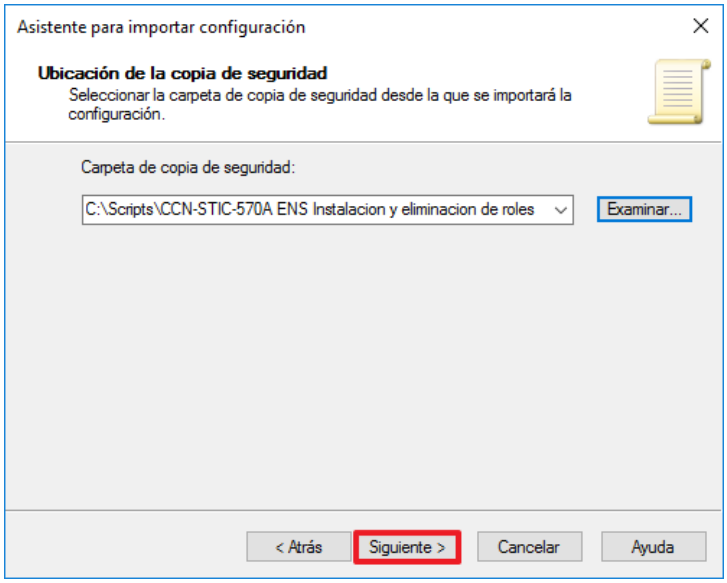
Las categorías media y alta de la presente guía deshabilitan la posibilidad de realizar la instalación remota de roles, características y servicios de rol a través de Shell.

Windows Server 2016 presenta unos mecanismos de administración que operan sobre el servidor local como si de un servidor remoto se tratara. Este hecho provoca la imposibilidad de instalar roles, características o servicios de rol adicionales sin modificar la plantilla de seguridad.

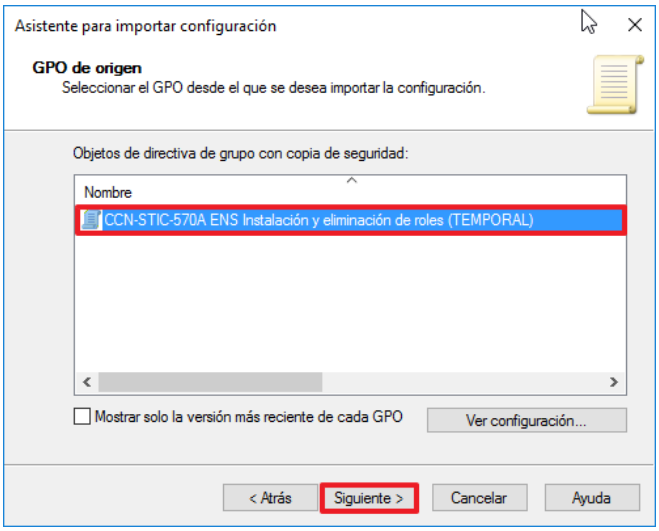
Por tanto y para posibilitar la instalación de estos elementos, será necesario hacer una modificación en el servidor en el que se quieren instalar roles, características o servicios de rol adicionales.

Paso	Descripción
1.	Para la instalación de roles, características y servicios de rol adicionales en un servidor miembro o un controlador de dominio, deberá editar la directiva correspondiente en el controlador de dominio. Inicie la herramienta de "Administración de directivas de grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"** 
2.	Ubíquese sobre el nodo "Objetos de directiva de grupo" ubicado en **"Bosque:<su dominio> → Dominios → <su dominio> → Objetos de directiva de grupo"**. 

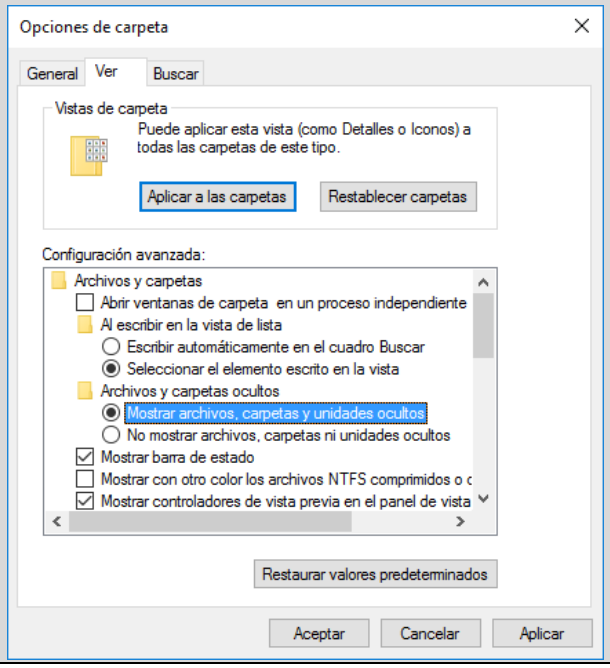
Paso	Descripción
3.	Pulse con el botón derecho, sobre dicha carpeta y seleccione la opción “Nuevo”. 
4.	Introduzca como nombre “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)” y pulse el botón “Aceptar”. 
5.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración…”. 
6.	En el asistente de importación de configuración, pulse el botón “Siguiente >”.
7.	En “Carpeta de copia de seguridad”, pulse el botón “Examinar...”.

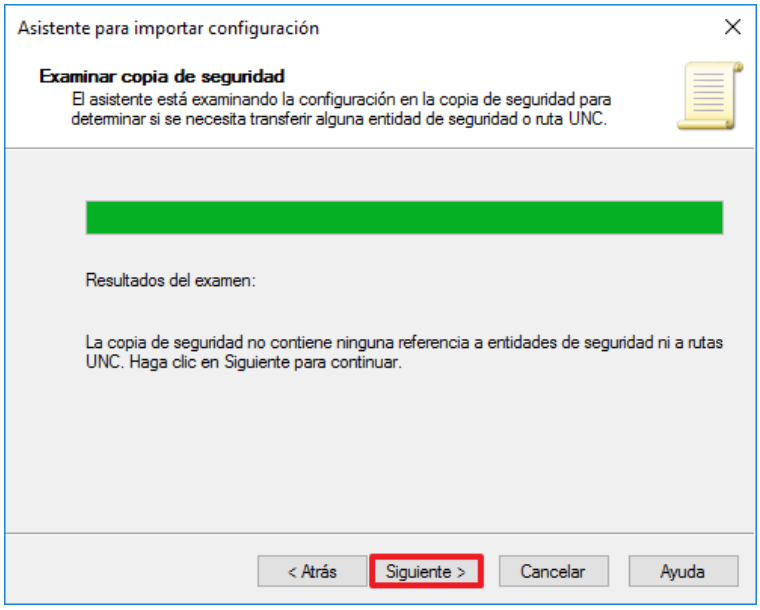
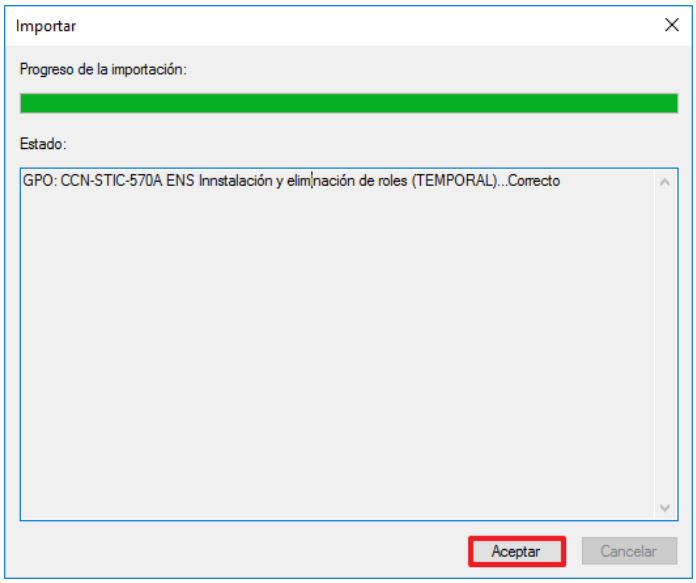
Paso	Descripción
8.	Seleccione la carpeta “CCN-STIC-570A ENS Instalación y eliminación de roles” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 
9.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada. 

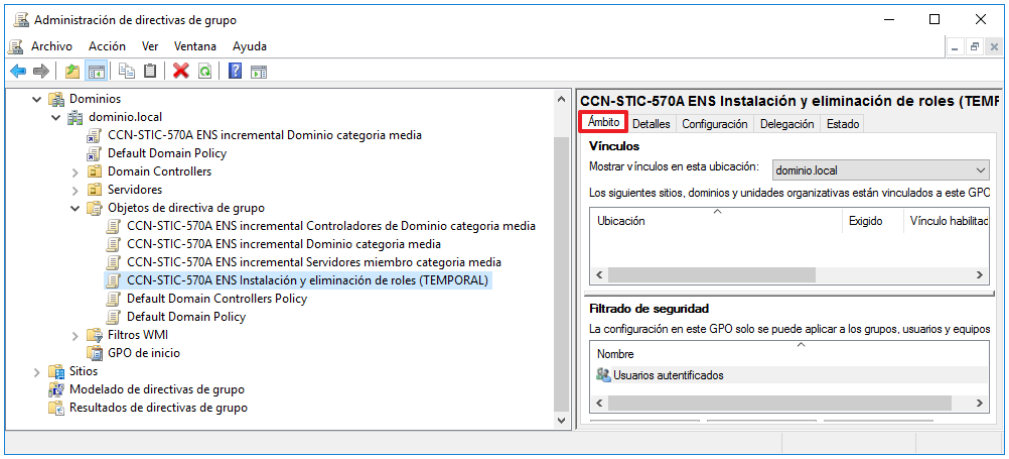
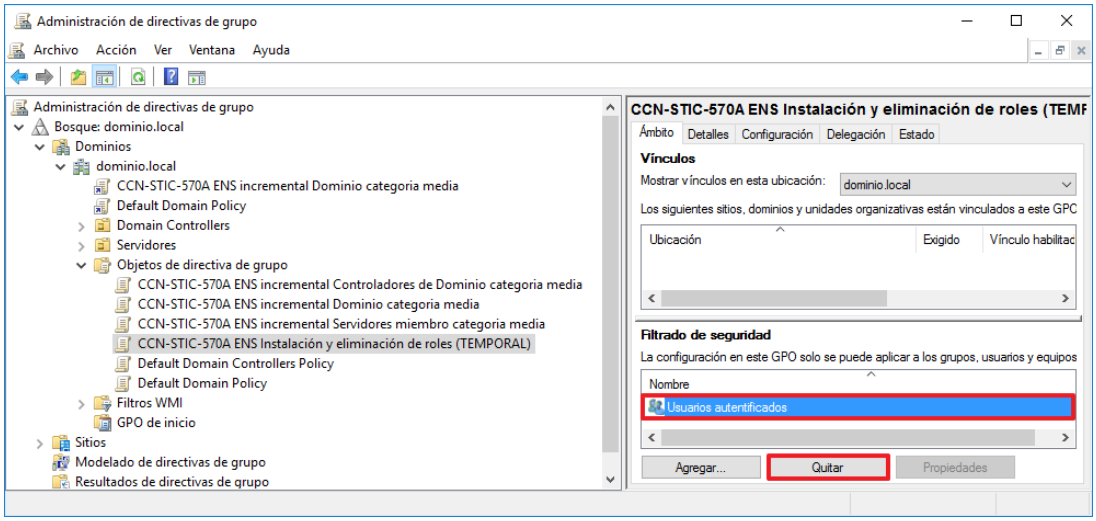
Paso	Descripción
10.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)” y pulse el botón “Siguiente >”.

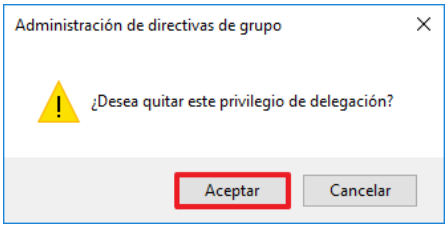
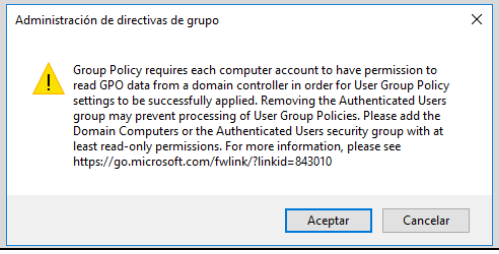
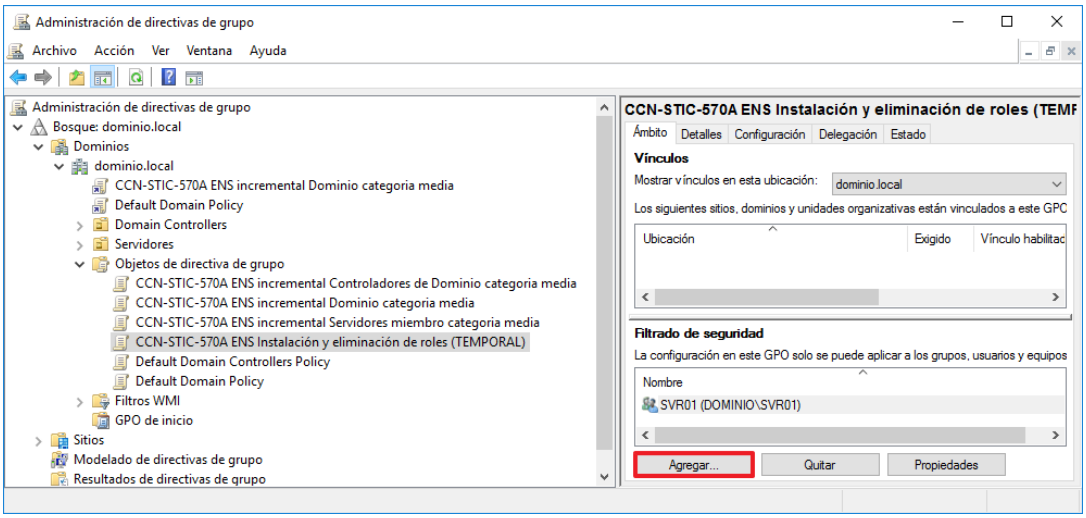


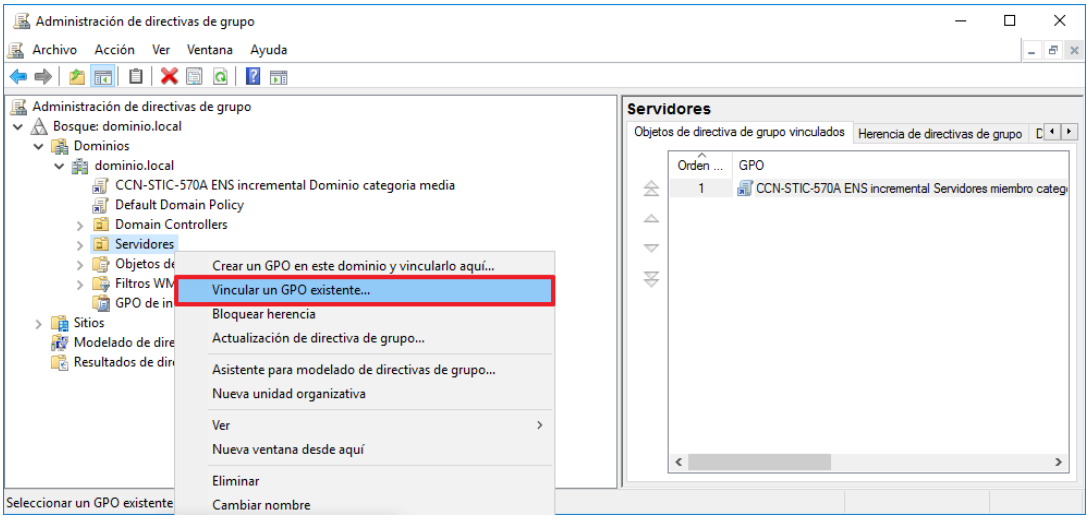
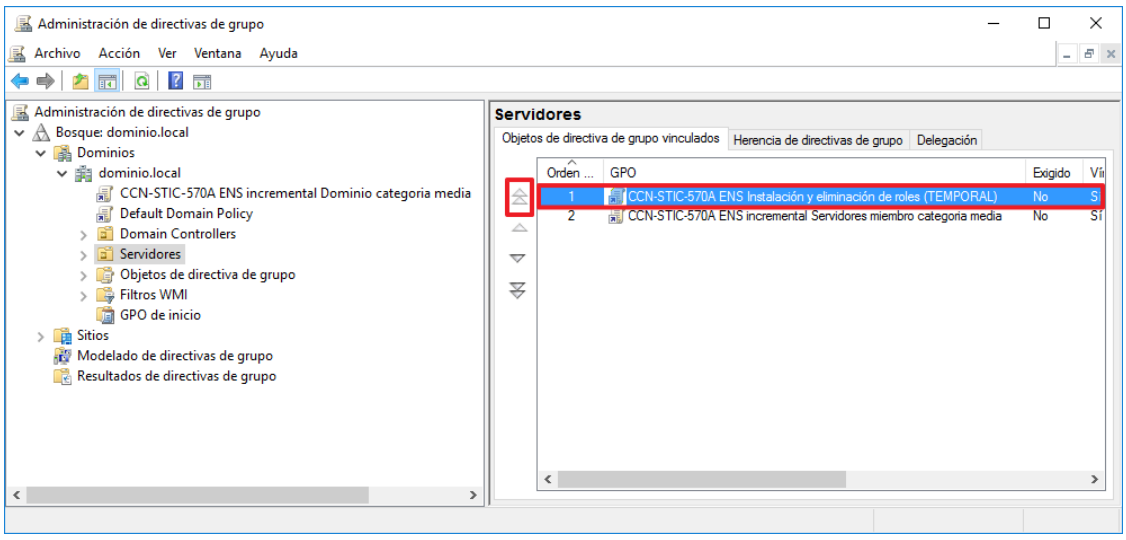
Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero “manifest.xml”. Este es un fichero oculto y, por lo tanto, debe mostrar en “opciones de carpeta” la opción “Mostrar archivos, carpetas y unidades ocultos”.



Paso	Descripción
11.	En la pantalla de examen, pulse el botón “Siguiente >”. 
12.	Para completar el asistente pulse el botón “Finalizar”.
13.	Cierre el asistente pulsando el botón “Aceptar”. 

Paso	Descripción
14.	A continuación, seleccione la nueva política de grupo configurada y diríjase a la pestaña “Ámbito” que se encuentra en el panel derecho. 
15.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 

Paso	Descripción
16.	A continuación, pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación.  **Nota**: Si aparece la siguiente advertencia ignórela y pulse “Aceptar”. 
17.	Una vez quitado, pulse el botón “Agregar…” y seleccione únicamente los equipos o grupos sobre los que desea aplicar la política de seguridad.  **Nota**: En este ejemplo se agrega el equipo SVR01.

Paso	Descripción
18.	A continuación, identifique las unidades organizativas en la que desea instalar o eliminar algún rol y/o característica. Pulse con el botón derecho sobre la unidad organizativa deseada y seleccione la opción del menú contextual “Vincular un GPO existente…”.  **Nota**: En este ejemplo se selecciona la unidad organizativa “Servidores”.
19.	Una vez vinculado, en el panel derecho seleccione la pestaña “Objetos de directiva de grupo vinculados” y seleccione la política “CCN-STIC 570A ENS Instalación y eliminación de roles (TEMPORAL)”
20.	Pulse el botón con la flecha que apunta hacia arriba hasta situar la política “CCN-STIC 570A ENS Instalación y eliminación de roles” en primer lugar dentro del orden de vinculación. 

Paso	Descripción
21.	Elimine el directorio “C:\Scripts”. **Nota:** Debe tener en consideración que ha alterado la política relativa a la configuración remota mediante Shell y ésta, al ser menos rigurosa que la propuesta en la configuración deseada de esta guía, se encuentra por debajo de los requerimientos de seguridad actuales. Una vez instalados los roles, características o servicios de rol necesarios, debería desvincular y/o eliminar la GPO “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)”.