CCN
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 570B

IMPLEMENTACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD EN WINDOWS SERVER 2016 (SERVIDOR INDEPENDIENTE)

NOVIEMBRE 2018

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2018.11.29 15:28:25 +01'00'

NIPO: 083-19-033-5
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 SERVIDOR INDEPENDIENTE

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 la implantación de condiciones de seguridad en las infraestructuras y servicios sujetos al RD 3/2010 y que se encontraran 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 los niveles, qué mecanismos se deberán habilitar para su cumplimiento. Habida cuenta de esta información, a continuación, se detallarán las diferentes plantillas de seguridad aplicables en función de 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. Estás, por las condiciones de aplicación de escenario de servidor independiente, se generarán como cuentas locales en los servidores. Dichas cuentas deberán ser gestionadas de tal forma que puedan 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 los privilegios asignados por membresía a grupo o los específicamente consignados para el acceso a servicios y aplicaciones existentes en el servidor.

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 de igual modo aplicable a sistemas Windows Server 2016. Aunque será mencionada a lo largo de la presente guía, en relación a todas las acciones enfocadas a garantizar la trazabilidad, se recoge específicamente la capacidad para la segregación de auditoría de registros empleados en Windows Server 2016 y sus servicios, a través del sistema de Suscripción de eventos con el que Microsoft ya dotó a Windows Server 2008.

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.

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 este 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.

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

c) 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 exigida.

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. 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 articula la aplicación de mecanismos de índole tecnológica y otros de tipo físico. Entre estos últimos, pueden localizarse los 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 son de completa aplicación. Por ejemplo, la necesidad de realizar un bloqueo del puesto de trabajo.

1.2.1.2. 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 locales.

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 que les 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 situadas 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 locales, 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	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 B.7 de la guía CCN-STIC-570A, adaptándolos a la organización.
OP. ACC. 4	Control de cuentas de usuario	Implementación de LGPO a través de plantillas facilitadas en la presente guía.
OP. ACC. 5	Política de contraseñas	Implementación de LGPO a través de plantillas facilitadas en la presente guía.
OP. ACC. 5	Protocolos de autenticación local	Implementación de LGPO a través de plantillas facilitadas en la presente guía.

Control	Medida	Mecanismo de aplicación
OP. ACC. 6	Bloqueo de cuentas	Implementación de LGPO a través de plantillas facilitadas en la presente guía.
OP. ACC. 7	Protocolos de autenticación en red	Implementación de LGPO 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 LGPO 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 LGPO a través de plantillas facilitadas en la presente guía.
OP. EXP. 4	Mantenimiento del Sistema Operativo	Implementación de LGPO 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 LGPO a través de plantillas facilitadas en la presente guía.
MP. COM. 3	Protección del sistema mediante implementación de firewall.	Implementación de LGPO a través de plantillas facilitadas en la presente guía. Implementación de configuración de firewall avanzado a nivel local según ANEXO A.5.1 en la presente guía.
MP. COM. 3	Protección de la autenticación.	Implementación de LGPO a través de plantillas facilitadas en la presente guía.

ANEXO A.2. CATEGORÍA BÁSICA

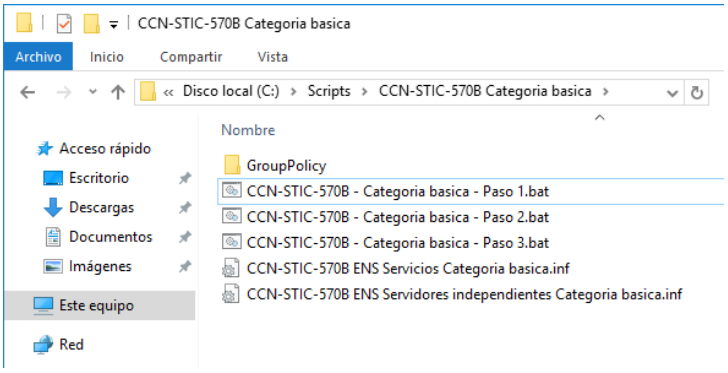
ANEXO A.2.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE WINDOWS SERVER 2016 COMO SERVIDOR INDEPENDIENTE PARA LA CATEGORÍA BÁSICA

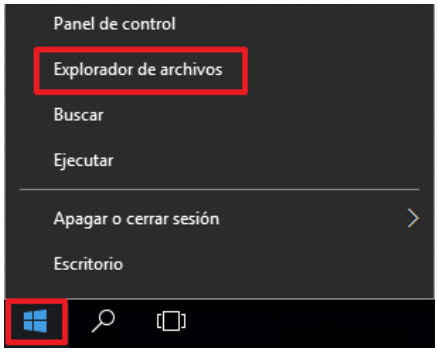
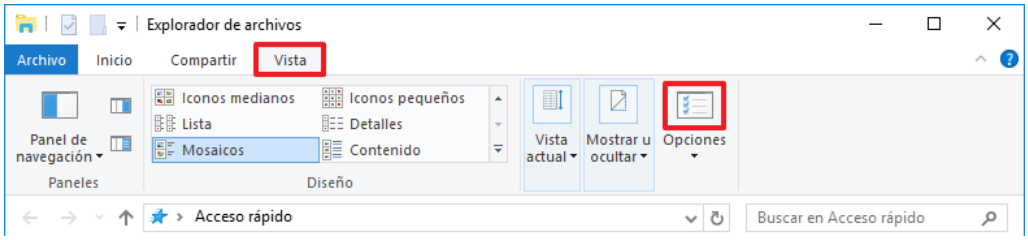
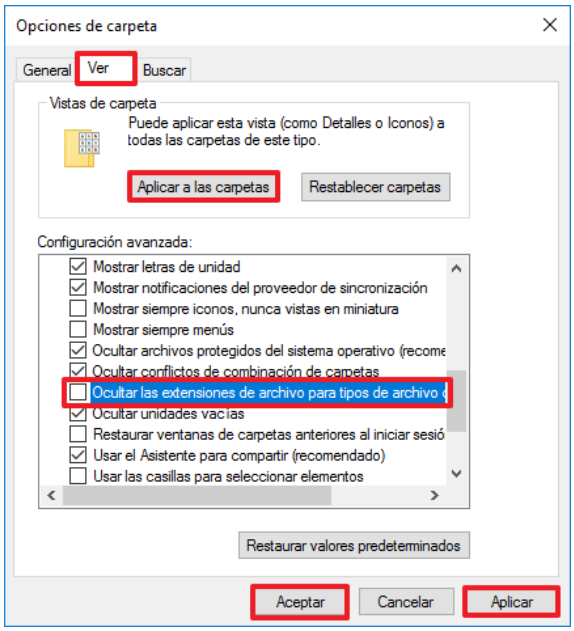
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se emplee Windows Server 2016, con una categorización de seguridad baja, según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación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

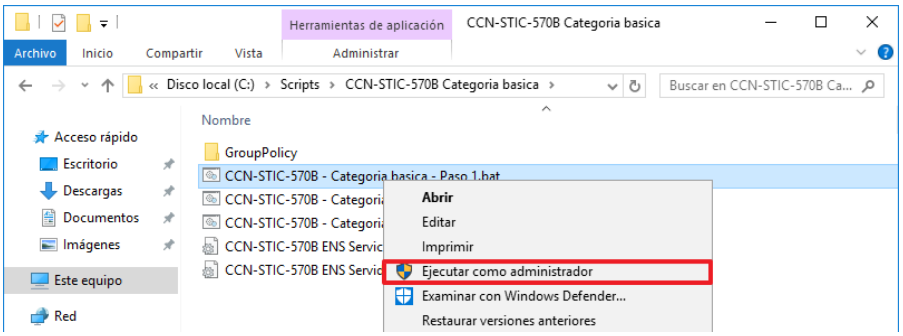
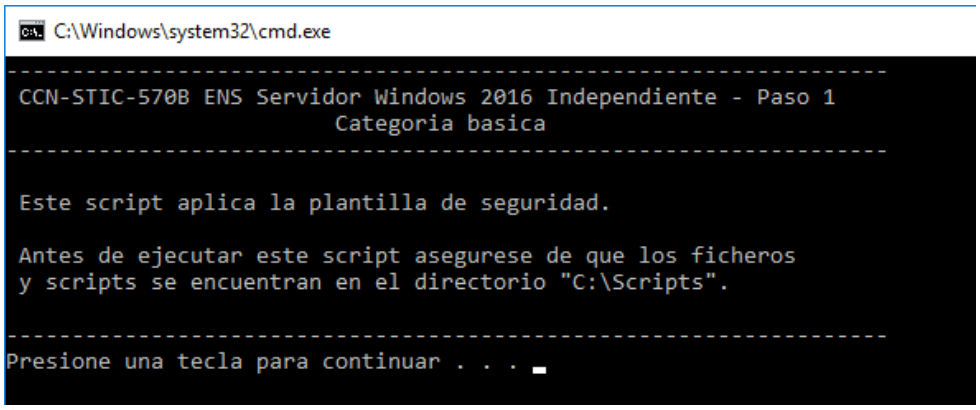
Se debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, será necesaria la realización de pruebas, en un entorno de preproducción, con objeto de familiarizarse con el escenario y comprobar la funcionalidad.

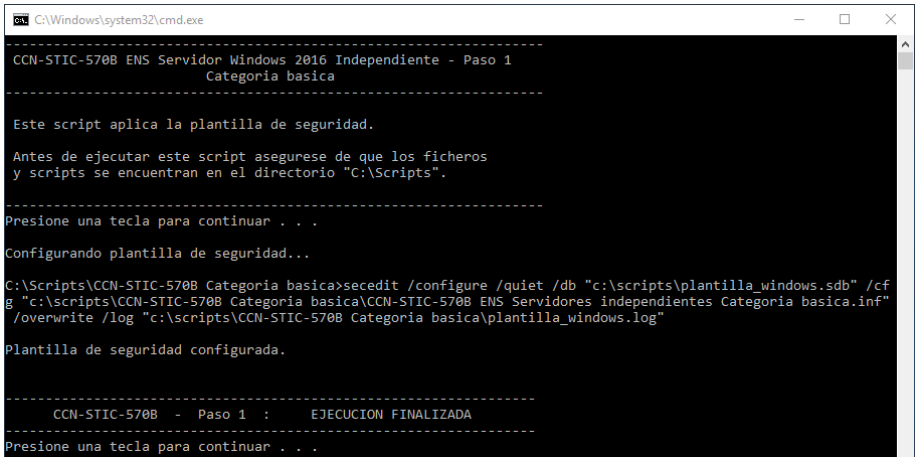
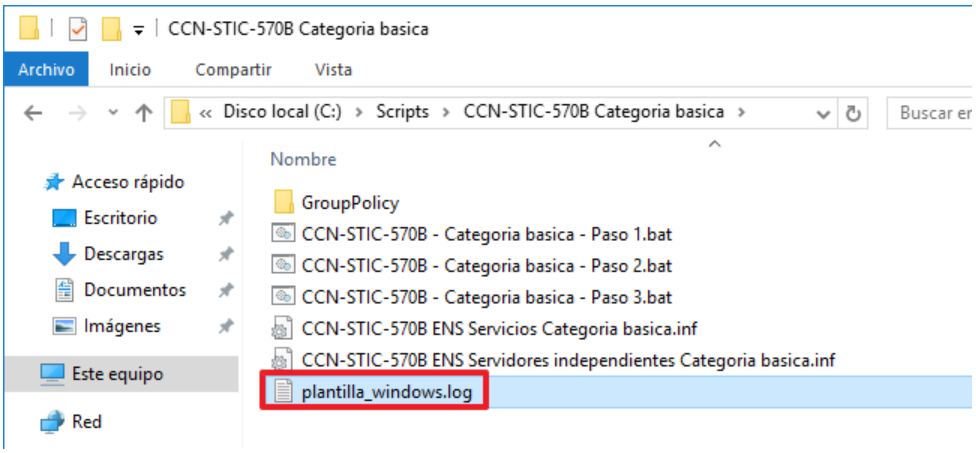
1. CONFIGURACIÓN DE LA SEGURIDAD LOCAL

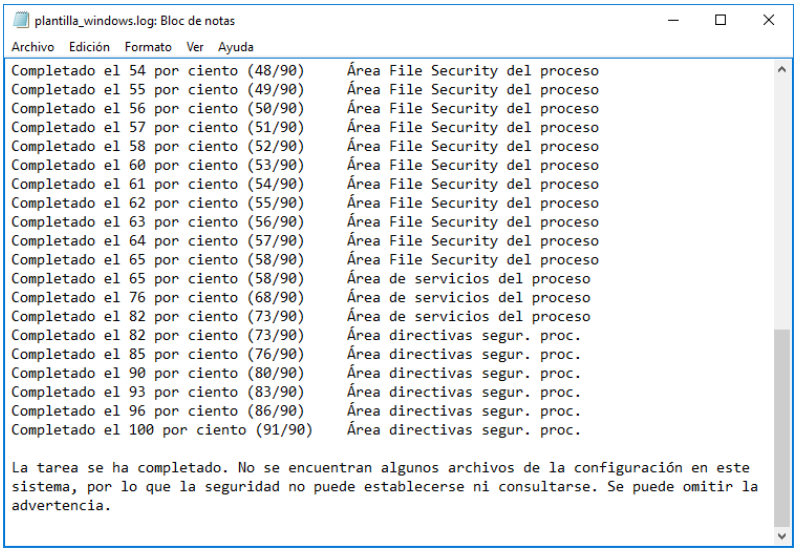
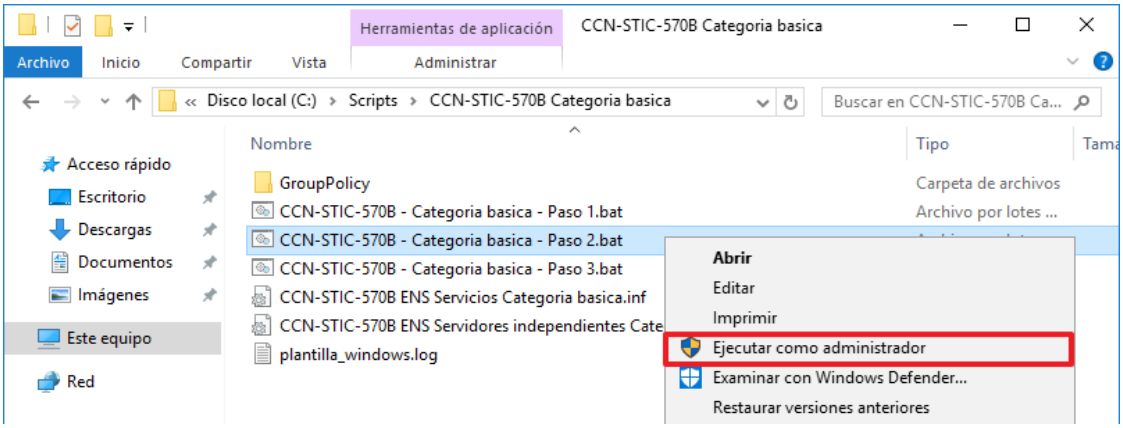
Los pasos que se describen a continuación se realizarán en todos aquellos servidores Windows Server 2016, independientes a un dominio, que implementen servicios o información de categoría básica y que se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

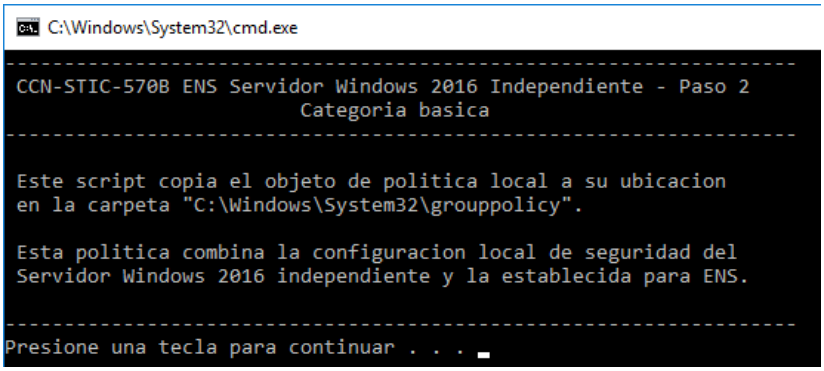
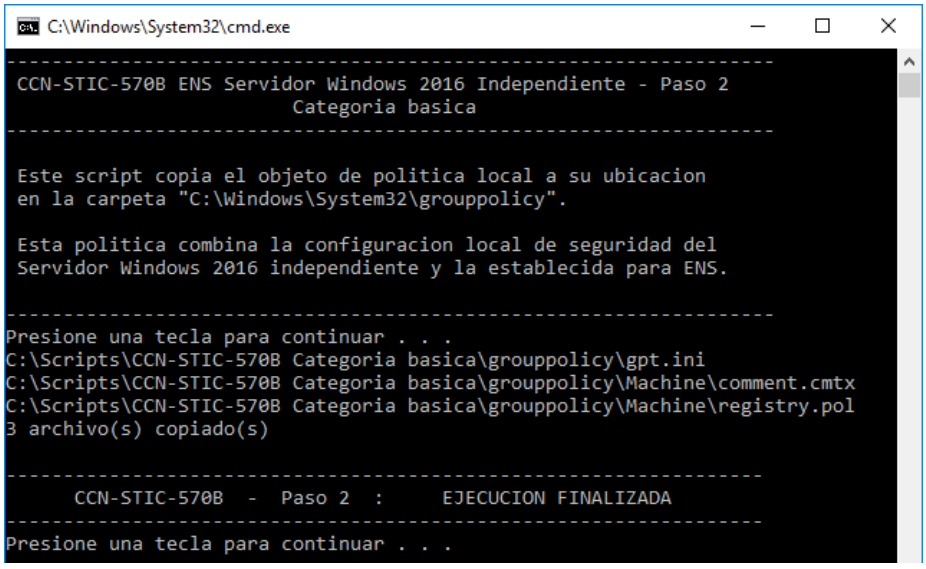
Paso	Descripción
1.	Inicie sesión en el servidor independiente donde se va aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del servidor.
3.	Cree el directorio “Scripts” en la unidad “C:\”.
4.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.
5.	Abra la carpeta “CCN-STIC-570B Categoria basica” que encontrará en la carpeta “C:\Scripts” que ha copiado. 

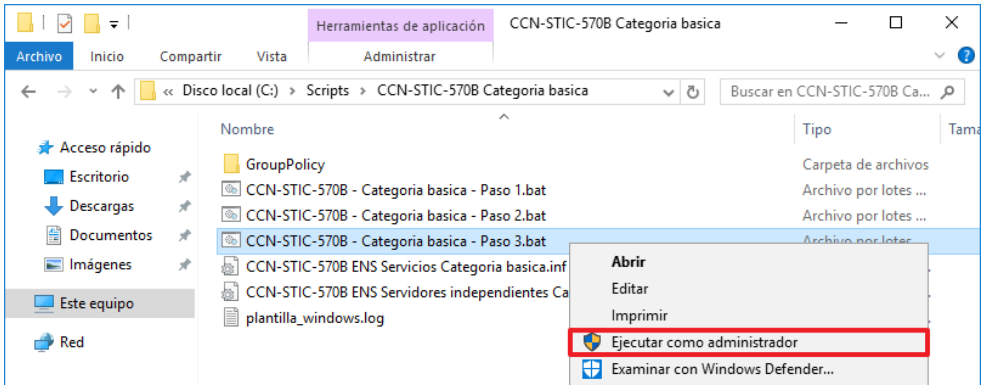
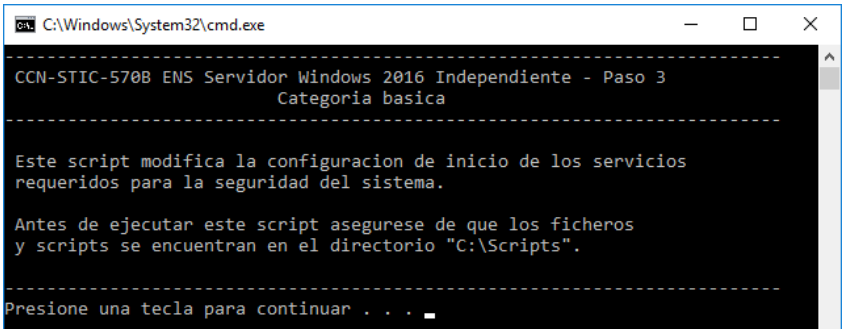
Paso	Descripción
6.	Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de “Inicio” con el botón derecho y seleccione “Explorador de archivos”. 
7.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”. 
8.	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”. 

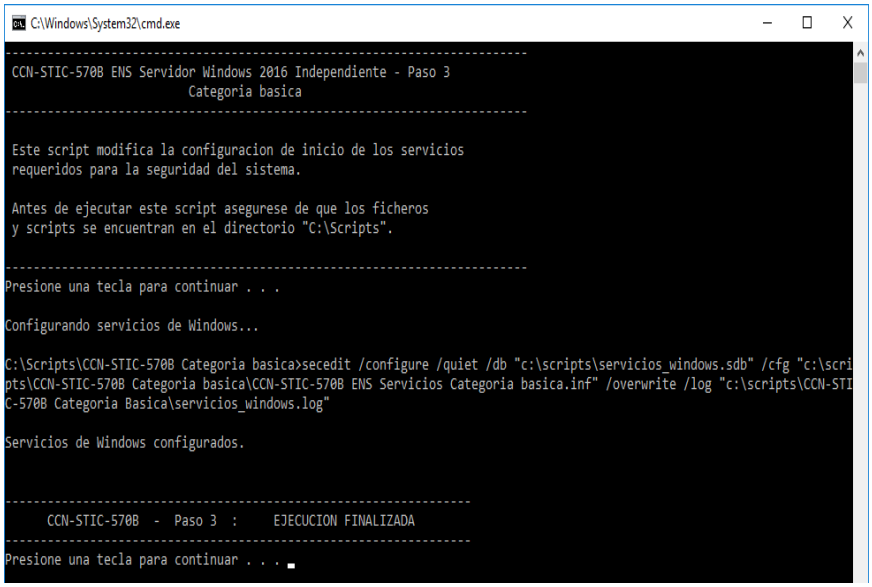
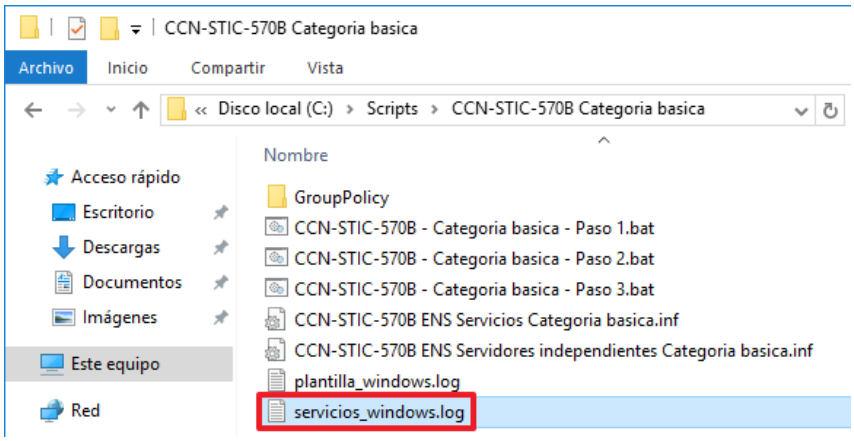
Paso	Descripción
9.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio. – GroupPolicy (directorio) – CCN-STIC-570A Categoria basica – Paso 1.bat – CCN-STIC-570A Categoria basica – Paso 2.bat – CCN-STIC-570A Categoria basica – Paso 3.bat – CCN-STIC-570A ENS Servicios Categoria basica.inf – CCN-STIC-570A ENS Servidores independientes Categoria basica.inf
10.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-570B – Categoria basica – Paso 1.bat” y seleccione la opción “Ejecutar como administrador”.  **Nota:** En función del usuario administrador con el que haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que le solicite elevación de privilegios, introducir credenciales de la cuenta del usuario con los privilegios de administrador o bien eleve automáticamente los privilegios sin solicitarle nada.
11.	Pulse una tecla para iniciar la ejecución del script que configurará la plantilla de seguridad con la seguridad requerida para la categoría básica del ENS. 

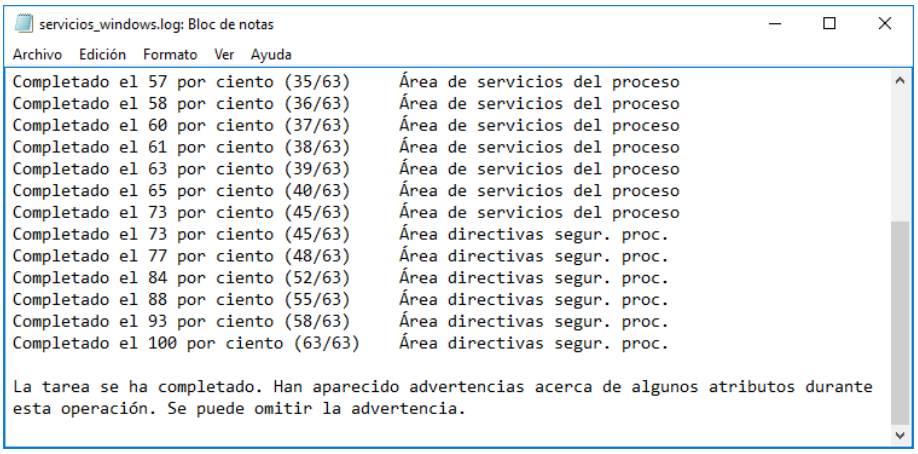
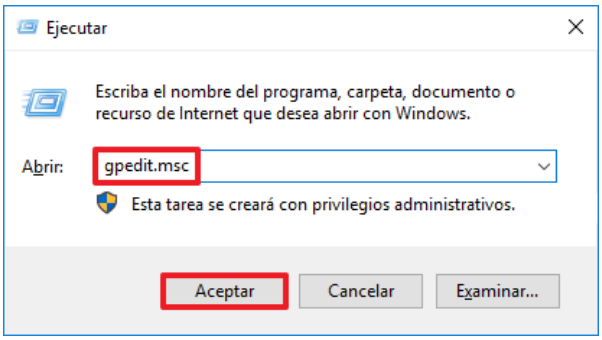
Paso	Descripción
12.	Una vez completado el proceso, deberá pulsar una tecla para continuar. 
13.	Pulse de nuevo otra tecla, para finalizar la ejecución del script. La ejecución del script genera un registro en la carpeta “C:\Scripts\CCN-STIC-570B Categoria basica” con el nombre de “plantilla_windows.log”. 

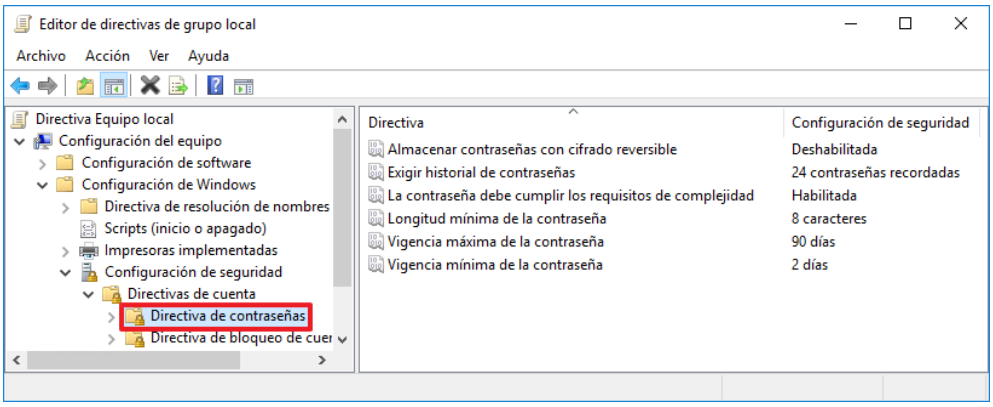
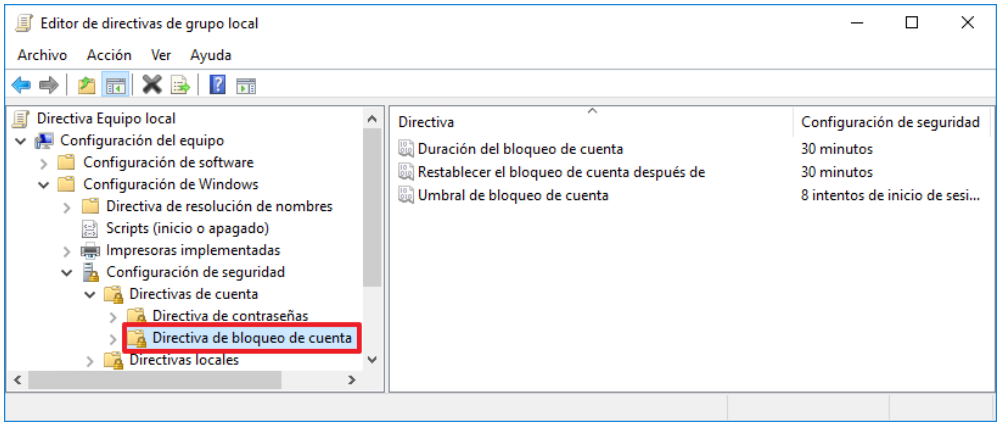
Paso	Descripción
14.	Abra este registro para comprobar si la configuración de la plantilla ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  **Nota:** En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script desde el paso 10.
15.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-570B – Categoria basica – Paso 2.bat” y seleccione la opción “Ejecutar como administrador”.  **Nota:** En función del usuario administrador con el que haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que le solicite elevación de privilegios, introducir credenciales de la cuenta del usuario con los privilegios de administrador o bien eleve automáticamente los privilegios sin solicitarle nada.

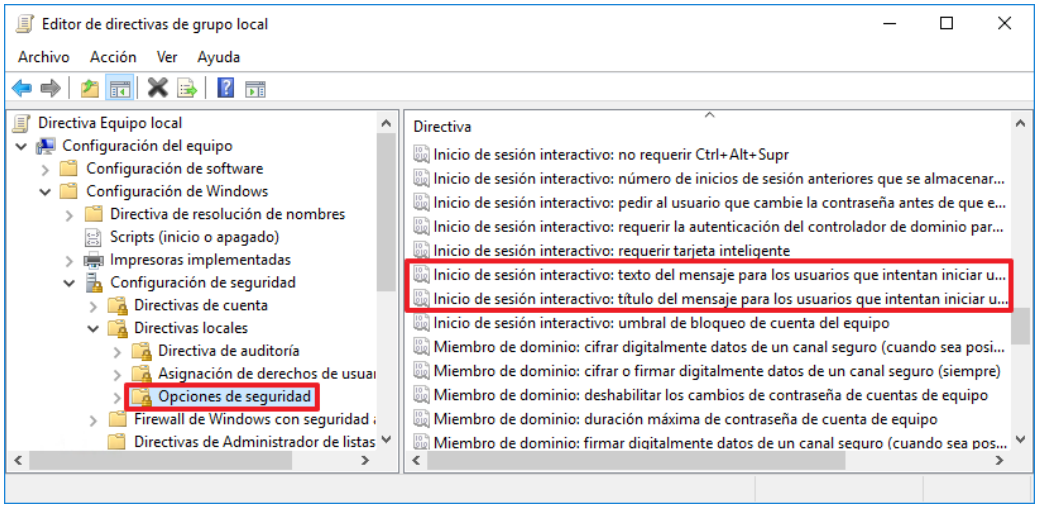
Paso	Descripción
16.	Pulse una tecla para iniciar la ejecución del script que configurará las plantillas administrativas con la seguridad requerida para la categoría básica del ENS. 
17.	Una vez completado el proceso, deberá pulsar una tecla para continuar. 

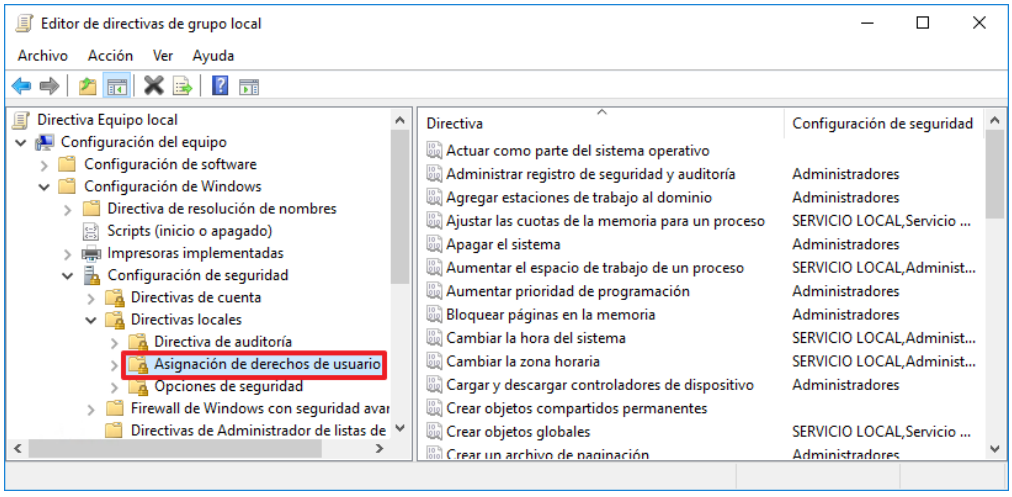
Paso	Descripción
18.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-570B – Categoria basica – Paso 3.bat” y seleccione la opción “Ejecutar como administrador”.  **Nota:** En función del usuario administrador con el que haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que le solicite elevación de privilegios, introducir credenciales de la cuenta del usuario con los privilegios de administrador o bien eleve automáticamente los privilegios sin solicitarle nada.
19.	Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la categoría básica del ENS. 

Paso	Descripción
20.	Una vez completado el proceso, deberá pulsar una tecla para continuar. 
21.	Pulse de nuevo otra tecla, para finalizar la ejecución del script. La ejecución del script genera un registro en la carpeta “C:\Scripts\CCN-STIC-570B Categoria basica con el nombre de “servicios_windows.log”. 

Paso	Descripción
22.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  **Nota:** En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script desde el paso 18.
23.	Es factible que su organización cuente con una política de contraseña consolidada. La implementación de la política de categoría básica implementará una específica para los servidores con categoría básica. Deberá evaluarla para determinar si esta configuración le es válida o por el contrario debe adaptarla a las condiciones de su organización.
24.	Inicie el “Editor de directivas de grupo local”. Para ello, vaya al menú “Ejecutar” y escriba “gpedit.msc” y pulse “Aceptar”. **“Tecla Windows + R → gpedit.msc”** 

Paso	Descripción
25.	Despliegue la política y sitúese en la siguiente ruta. **"Directiva Equipo Local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseña"** 
26.	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.
27.	De forma similar a lo anterior, deberá evaluar la política de bloqueo de cuenta. Para ello y sin cerrar el editor, seleccione la "Directiva de bloqueo de cuenta" que encontrará al mismo nivel que la directiva de contraseñas. 
28.	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.

Paso	Descripción
29.	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.
30.	Para informar de las obligaciones sitúese en la siguiente ruta. **"Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"**
31.	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". 
32.	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.

Paso	Descripción
33.	Por último, la política de seguridad local especifica 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 haya asignado derechos determinados para la administración o gestión de los sistemas. Si esto fuera así deberá realizar las modificaciones sobre la configuración de política local.
34.	Despliegue la política y sitúese en la siguiente ruta. **"Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"** 
35.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
36.	Cierre el "Editor de directivas de grupo local".
37.	Elimine la carpeta "C:\Scripts" y su contenido.
38.	Reinicie el servidor.

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

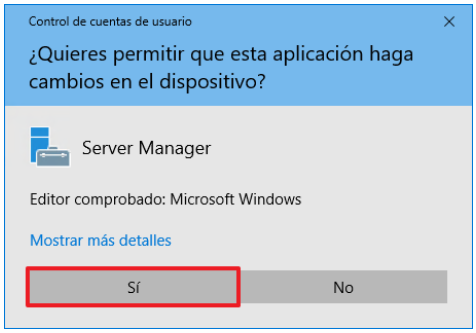
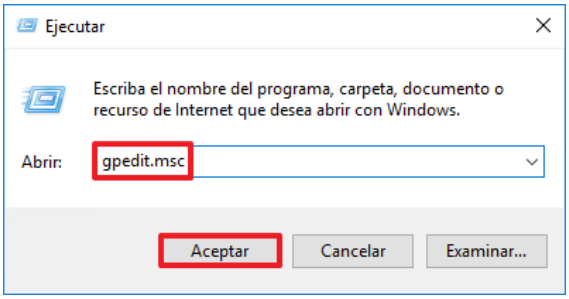
El control de cuentas de usuario surge, en Windows Vista, como respuesta para limitar las acciones de los administradores cuando actuaban con cuentas privilegiadas ante operativas que no requerían dicho privilegio. En sistemas previos a Windows Vista, un administrador que había iniciado una sesión actuaba 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.

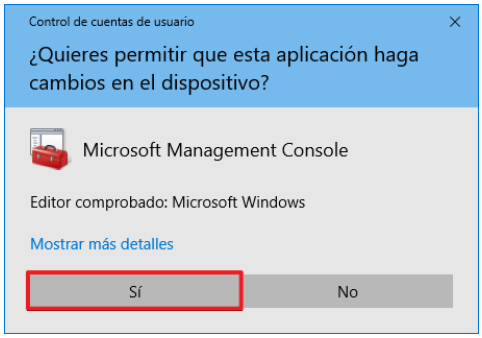
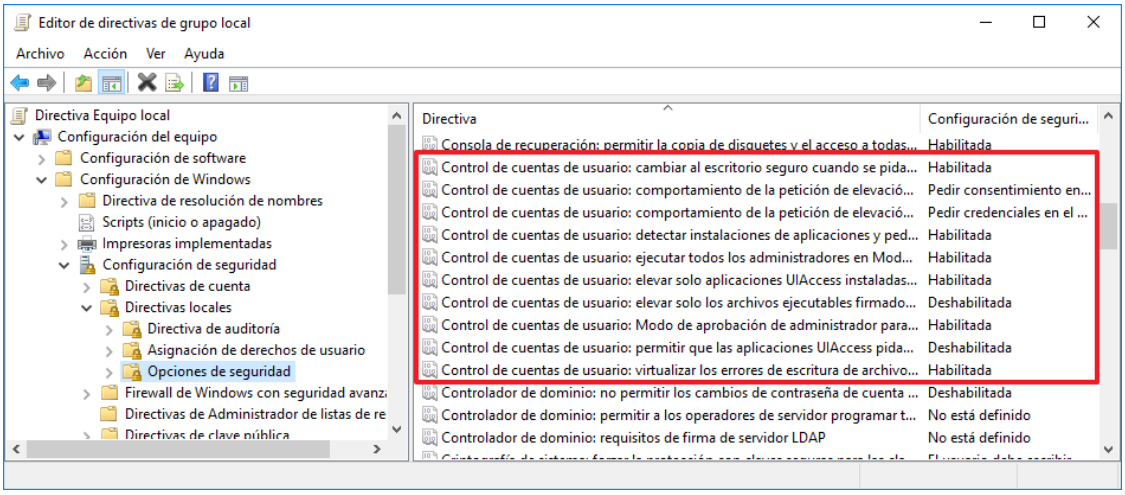
Siguiendo el principio de menor privilegio y menor exposición, la presente guía habilita las condiciones de funcionalidad de UAC para la categoría básica, aunque con los criterios más laxos de los aplicables.

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 modificación de la política local, de seguridad de aplicación a los servidores miembros, que pudieran presentar incidencias con la configuración de UAC.

Debe tenerse en cuenta 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.

Paso	Descripción
39.	Inicie sesión en el servidor independiente con una cuenta de administrador local. El sistema le solicitará elevación de privilegios para poder ejecutar la herramienta "Administrador del servidor". Pulse "Sí" para continuar. 
40.	Inicie el "Editor de directivas de grupo local". Para ello, vaya al menú "Ejecutar" y escriba "gpedit.msc" y pulse "Aceptar". **"Tecla Windows + R → gpedit.msc"** 

Paso	Descripción
41.	Pulse “Sí” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 
42.	Despliegue la política local y sitúese en la siguiente ruta. **“Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**
43.	Identifique las directivas relativas a “Control de cuenta de usuario”. 
44.	Realice las modificaciones oportunas.
45.	Cierre la política.
46.	Reinicie el servidor. **Nota:** Debe tener en consideración que, si ha alterado la política de control de cuentas y ésta es menos rigurosa que la propuesta en la configuración deseada de 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.2.2. LISTA DE COMPROBACIÓN DE WINDOWS SERVER 2016 COMO SERVIDOR INDEPENDIENTE 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 y para una configuración completa, se debe consultar el punto de la guía "ANEXO A.2.1 PASO A PASO DE IMPLEMENTACIÓN SEGURA DE WINDOWS SERVER 2016 COMO SERVIDOR INDEPENDIENTE PARA 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 servidores Windows Server 2016 independientes con implementación de seguridad de categoría básica del ENS.

Para realizar esta lista de comprobación, deberá iniciar sesión en el servidor con una cuenta de usuario que tenga privilegios de administrador local.

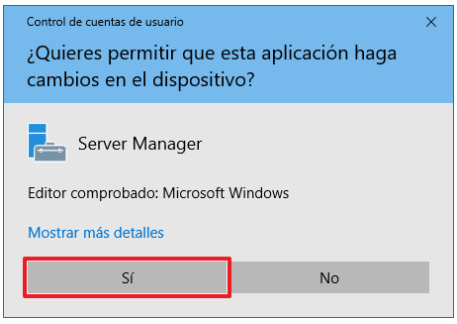
Para realizar las comprobaciones pertinentes en el servidor se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor. Las consolas y herramientas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

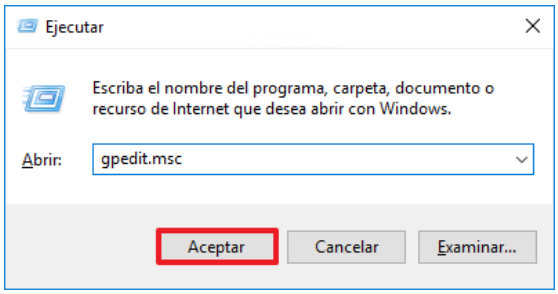
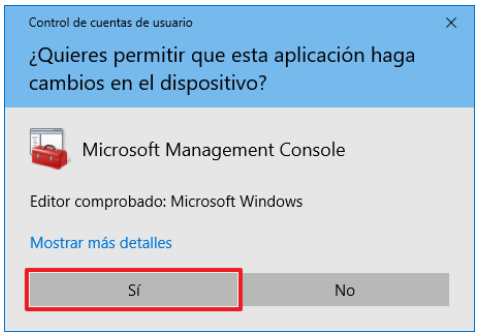
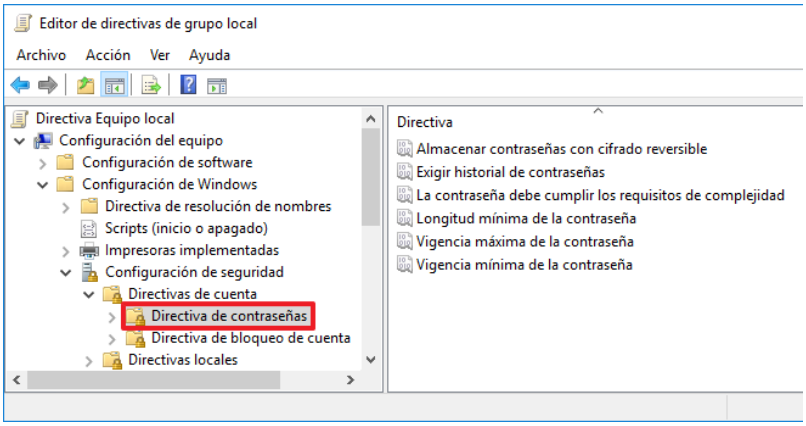
a) Editor de objetos de directiva de grupo local (gpedit.msc).

b) Editor de registro (regedit.exe).

c) Visor de Eventos (eventvwr.exe).

d) Servicios (services.msc).

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el servidor.		Inicie sesión en el servidor independiente con una cuenta de administrador local. El sistema le solicitará elevación de privilegios para poder ejecutar la herramienta "Administrador del servidor. Pulse "Sí" para continuar. 

Comprobación	OK/NOK	Cómo hacerlo
2. Verifique la directiva de contraseñas en el editor de objetos de directiva de grupo local.		Inicie el "Editor de directivas de grupo local". Para ello, vaya al menú ejecutar y escriba "gpedit.msc" y pulse "Aceptar". **"Tecla Windows + R → gpedit.msc"**  Pulse "Sí" cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo.  En el "Editor de objetos de directiva de grupo local" seleccione el siguiente nodo: **"Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de contraseñas"** 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="7"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Almacenar contraseñas usando cifrado reversible</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Exigir historial de contraseñas</td><td>24 contraseñas recordadas</td><td></td></tr>
<tr><td colspan="2">Las contraseñas deben cumplir los requisitos de complejidad</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Longitud mínima de la contraseña</td><td>8 caracteres</td><td></td></tr>
<tr><td colspan="2">Vigencia máxima de la contraseña</td><td>90 días</td><td></td></tr>
<tr><td colspan="2">Vigencia mínima de la contraseña</td><td>2 días</td><td></td></tr>
<tr><td rowspan="5">3. Verifique las directivas de bloqueo de cuenta en el editor de objetos de directiva de grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo local → Configuración del Equipo → 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>4. Verifique las directivas de auditoría en el editor de objetos de directiva de grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo local → Configuración del Equipo → 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="9"></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="12">5. Verifique la asignación de derechos de usuario en el editor de objetos de directiva de grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → 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>
<tr><td colspan="2">Cambiar la zona horaria</td><td>SERVICIO LOCAL, Administradores</td><td></td></tr>
<tr><td colspan="2">Cargar y descargar controladores de dispositivo</td><td>Administradores</td><td></td></tr>
<tr><td colspan="2">Crear objetos globales</td><td>Administradores, SERVICIO, SERVICIO LOCAL, Servicio de red</td><td></td></tr>
<tr><td colspan="2">Crear un archivo de paginación</td><td>Administradores</td><td></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Crear vínculos simbólicos	Administradores	
		Denegar el acceso a este equipo desde la red	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 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	
		Omitir comprobación de recorrido	Todos, SERVICIO LOCAL, Servicio de red, Administradores, Usuarios, Operadores de copia de seguridad, Windows Manager.	
		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	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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	
6. Verifique las opciones de seguridad en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo: **"Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"**		

Directiva	Valor	OK/NOK
Acceso a redes: modelo de seguridad y uso compartido para cuentas locales	Clásico: usuarios locales se autentican con credenciales propias	
Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red	Habilitada	
Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Habilitada	
Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Habilitada	
Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	Deshabilitada	
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	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		**Valor**	**OK/NOK**
Acceso a redes: rutas y subrutas del registro accesibles remotamente		System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\EventLog Software\Microsoft\OLAP Server Software\Microsoft\WindowsNT\CurrentVersion\Print Software\Microsoft\WindowsNT\CurrentVersion\Windows System\CurrentControlSet\Control\Content Index System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\Currente Version\Perflib System\CurrentControlSet\Services\SysmonLog	
Acceso a red: permitir traducción SID/nombre anónima		Deshabilitada	
Apagado: borrar el archivo de paginación de la memoria virtual		Deshabilitada	
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		Deshabilitada	
Auditoría: auditar el acceso de objetos globales del sistema		Deshabilitada	
Auditoría: auditar el uso del privilegio de copias de seguridad y restauración		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	

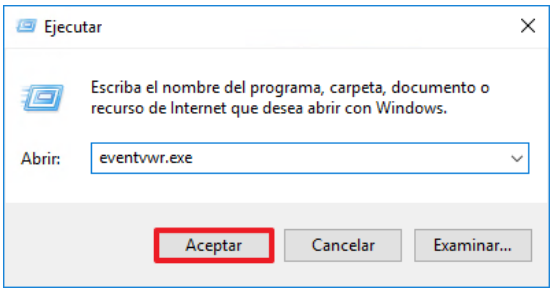
Comprobación	OK/NOK	Cómo hacerlo	
Directiva		**Valor**	**OK/NOK**
Configuración del sistema: usar reglas de certificado en ejecutables de Windows para directivas de restricción de software		Deshabilitada	
Consola de recuperación: permitir el inicio de sesión administrativo automático		Deshabilitada	
Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas		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: elevar solo aplicaciones UIAccess instaladas en ubicaciones seguras		Habilitada	
Control de cuentas de usuario: elevar solo los archivos ejecutables firmados y validados		Deshabilitada	
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 de Registro en diferentes ubicaciones por usuario		Habilitada	

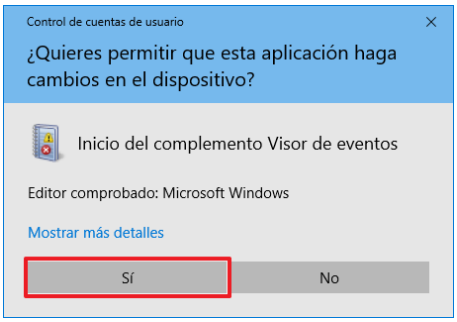
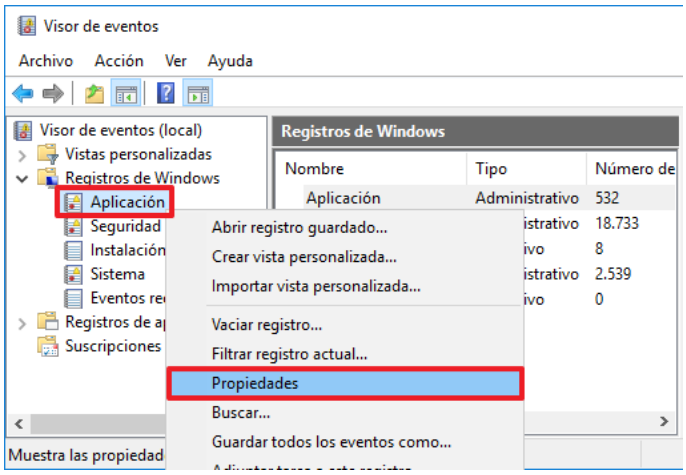
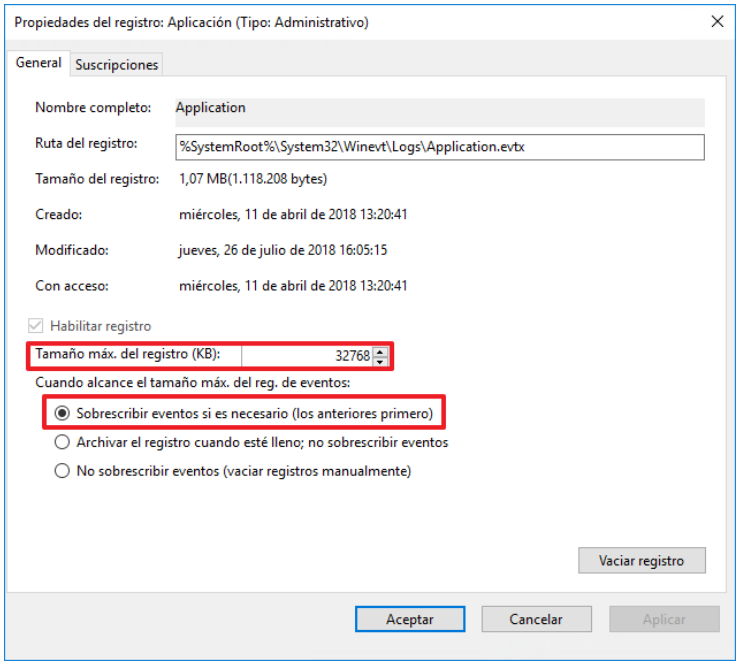
Comprobación	OK/NOK	Cómo hacerlo	
Directiva		**Valor**	**OK/NOK**
Controlador de dominio: no permitir los cambios de contraseña de cuenta de equipo		Deshabilitada	
Criptografía de sistema: Forzar la protección con claves seguras para las claves de usuario almacenadas en el equipo		El usuario debe escribir una contraseña cada vez que use una clave	
Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash		Deshabilitada	
Cuentas: cambiar el nombre de cuenta de invitado		Invitado	
Cuentas: cambiar el nombre de cuenta administrador		Administrador	
Cuentas: estado de la cuenta de administrador		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;;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		Habilitada	
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 a CD-ROM sólo al usuario con sesión iniciada localmente		Habilitada	
Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente		Bloquear estación de trabajo	

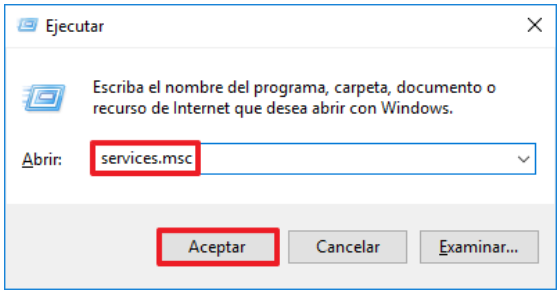
Comprobación	OK/NOK	Cómo hacerlo	
Directiva		**Valor**	**OK/NOK**
Inicio de sesión interactivo: mostrar información de usuario cuando se bloquee la sesión		No mostrar información del usuario	
Inicio de sesión interactivo: no mostrar el último nombre de usuario		Deshabilitada	
Inicio de sesión interactivo: 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	
Inicio de sesión interactivo: requerir la autenticación del controlador de dominio para desbloquear la estación de trabajo		Deshabilitada	
Inicio de sesión interactivo: requerir tarjeta inteligente		Deshabilitada	
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	
Objetos del sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que no sean de Windows		Habilitada	

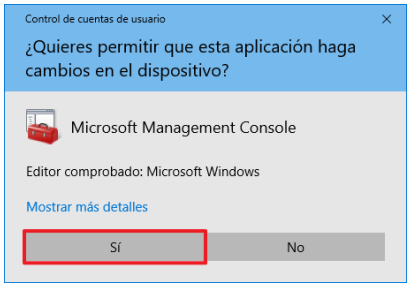
Comprobación	OK/NOK	Cómo hacerlo	
Directiva		**Valor**	**OK/NOK**
Seguridad de red: configurar tipos de cifrado permitidos para Kerberos		RC4_HMAC_MD5, AES128_HMAC_SHA1, AES2656_HMAC_SHA1, Tipos de cifrados futuros	
Seguridad de red: forzar el cierre de sesión cuando expire la hora de sesión		Deshabilitada	
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	
Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)		Requerir cifrado de 128 bits	
Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)		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	
de red Microsoft: firmar digitalmente las comunicaciones (siempre)		Deshabilitada	
Servidor de red de Microsoft: nivel de validación de nombres de destino SPN del servidor		Aceptar si lo proporciona el cliente	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td colspan="2">Directiva</td><td colspan="2">Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión</td><td colspan="2">30 minutos</td><td></td></tr>
<tr><td rowspan="4">7. Verifique las directivas del almacén digital en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → Plantillas administrativas → 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="4"></td></tr>
<tr><td rowspan="4">8. Verifique las directivas del informe de errores de Windows en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Configuración del Equipo → Plantillas Administrativas → 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>9. Verifique la configuración de la comunicación de Internet en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → Plantillas Administrativas → Sistemas → 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 rowspan="12"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Desactivar informe de errores de reconocimiento de escritura a mano</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar el Programa para la mejora de la experiencia</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar los vínculos “Events.asp” del Visor de eventos</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar el contenido “¿Sabía que…? Del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar la búsqueda en Microsoft Knowledge Base del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar el informe de errores de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar la actualización de archivos de contenido del Asistente para búsqueda</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar el acceso a la tienda</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar la tarea de imágenes “Pedir copias fotográficas”</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger</td><td>Habilitada</td><td></td></tr>
<tr><td></td><td></td><td colspan="3"></td></tr>
<tr><td>10. Verifique la configuración del registro de eventos en el editor de objetos de directiva de grupo local.</td><td></td><td colspan="3">Inicie el “Visor de eventos”. Para ello, vaya al menú ejecutar, escriba “eventvwr.exe” y pulse “Aceptar”.
“Tecla Windows + R →eventvwr.exe”
 
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
		El "Control de cuentas de usuario" solicitará elevación de privilegios. Pulse "Sí" para continuar.  En el "Visor de eventos" despliegue el contenedor "Registros de Windows" y seleccione propiedades haciendo clic derecho sobre "Aplicación".   Repita el proceso para "Seguridad" y "Sistema".

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="8"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Cuando alcance el tamaño máximo del registro de eventos de la aplicación</td><td>Sobrescribir eventos si es necesario (los anteriores primero)</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">Cuando alcance el tamaño máximo del registro de eventos de seguridad</td><td>Sobrescribir eventos si es necesario (los anteriores primero)</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">Cuando alcance el tamaño máximo del registro de eventos del sistema</td><td>Sobrescribir eventos si es necesario (los anteriores primero)</td><td></td></tr>
<tr><td colspan="2">Tamaño máximo del registro del sistema</td><td>32768 kilobytes</td><td></td></tr>
<tr><td>11. Verifique el modo de configuración de los servicios del sistema</td><td></td><td colspan="3">Inicie la consola de “Servicios”. Para ello, vaya al menú ejecutar, escriba “services.msc” y pulse “Aceptar”.
“Tecla Windows + R →services.msc”
 
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
		El "Control de cuentas de usuario" solicitará elevación de privilegios. Pulse "Sí" para continuar.  **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		
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado		
Adaptador de rendimiento de WMI	wmiApSrv	Manual		
Administración de aplicaciones	AppMgmt	Manual		
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado		
Administración de capas de almacenamiento	TieringEngineService	Manual		
Administración remota de Windows (WS-Management)	WinRM	Automático		
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual		
Administrador de conexiones de acceso remoto	RasMan	Manual		
Administrador de conexiones de Windows	Wcmsvc	Automático		
Administrador de configuración de dispositivos	DsmSvc	Manual		
Administrador de credenciales	VaultSvc	Manual		

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

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Ayudante especial de la consola de administración	sacsvr	Manual		
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual		
Captura SNMP	SNMPTRAP	Deshabilitado		
CDPUserSvc	CDPUserSvc	Automático		
Cliente de directiva de grupo	gpsvc	Automático		
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático		
Cliente DHCP	Dhcp	Automático		
Cliente DNS	Dnscache	Automático		
Cola de impresión	Spooler	Automático		
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Manual		
Comprobador puntual	svsvc	Manual		
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado		
Conexiones de red	Netman	Manual		
Configuración automática de redes cableadas	dot3svc	Manual		
Configuración de Escritorio remoto	SessionEnv	Manual		
Conjunto resultante de proveedor de directivas	RSoPProv	Manual		
Contenedor de Microsoft Passport	NgcCtnrSvc	Manual		
Coordinador de transacciones distribuidas	MSDTC	Automático		
CoreMessaging	CoreMessagingRegistrar	Automático		
DataCollectionPublishingService	DcpSvc	Manual		
Datos de contactos	PimIndexMaintenanceSvc	Manual		
Detección de hardware shell	ShellHWDetection	Deshabilitado		
Detección de servicios interactivos	UI0Detect	Manual		
Detección SSDP	SSDPSRV	Deshabilitado		

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

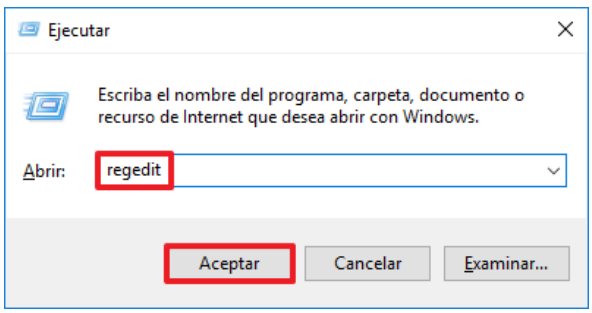
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Instrumental de administración de Windows	Winmgmt	Automático		
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual		
KTMRM para DTC (Coordinador de transacciones distribuidas)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

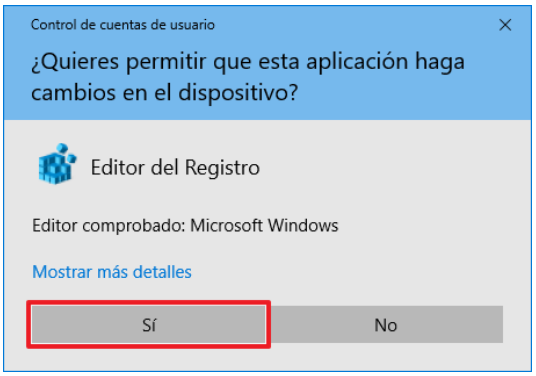
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService	Manual		
Registro de eventos de Windows	EventLog	Automático		
Registro remoto	RemoteRegistry	Deshabilitado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

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

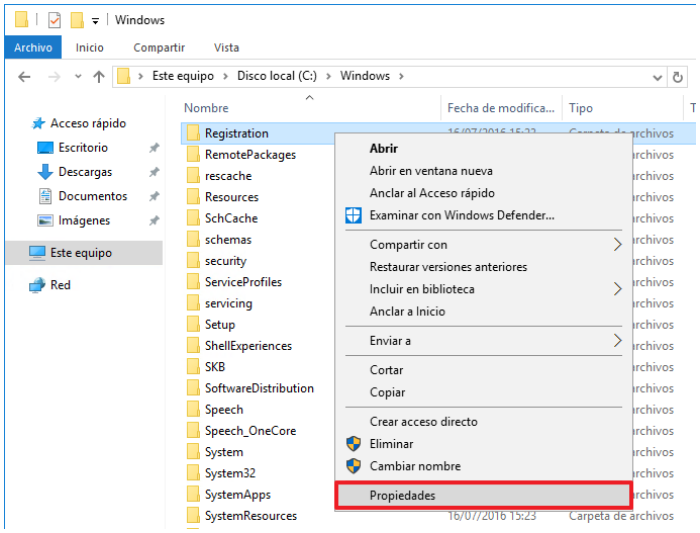
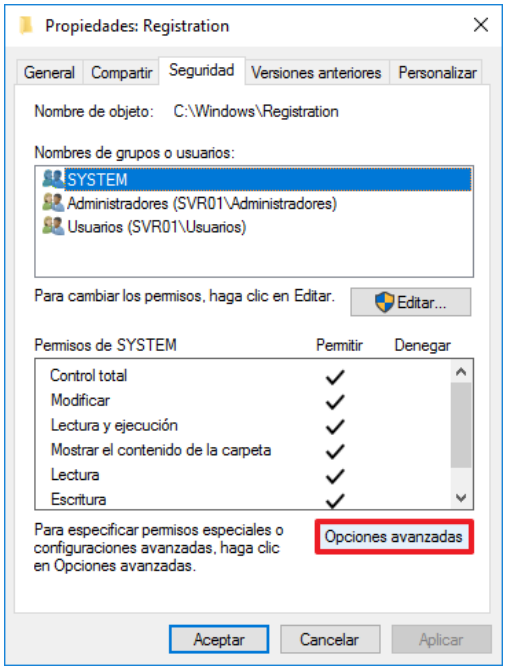
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService	Deshabilitado		
Servicio de perfil de usuario	ProfSvc	Automático		
Servicio de plataforma de dispositivos conectados	CDPSvc	Automático		
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Manual		
Servicio de puerta de enlace de nivel de aplicación	ALG	Manual		
Servicio de registro de acceso de usuarios	UALSVC	Automático		
Servicio de repositorio de estado	StateRepository	Manual		
Servicio de sensores	SensorService	Manual		
Servicio de servidor proxy KDC (KPS)	KPSSVC	Manual		
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual		
Servicio de supervisión de licencias de Windows	WLMS	Automático		
Servicio de supervisión de sensores	SensrSvc	Manual		
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Manual		
Servicio de uso compartido de datos	DsSvc	Manual		
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Deshabilitado		
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Manual		

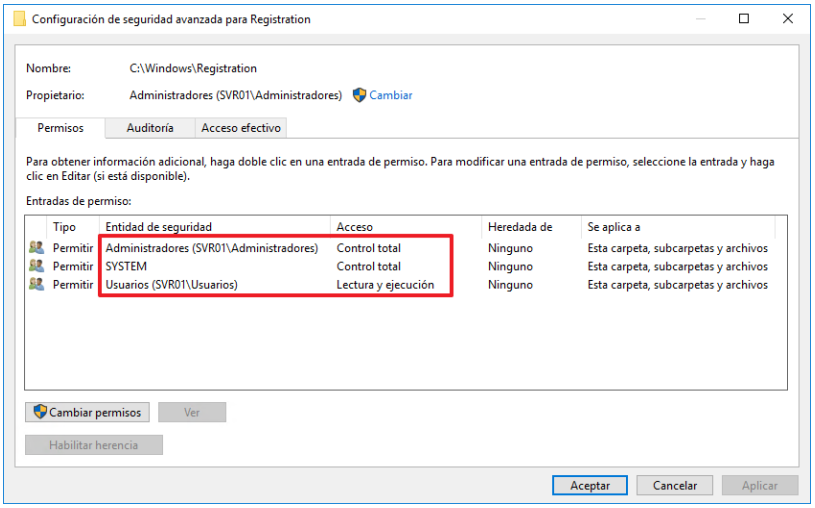
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual		
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado		
Servicio de Windows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

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servidor del modelo de datos del mosaico		tiledatamodelsvc	Automático		
Sincronizar host		OneSyncSvc	Automático		
Sistema de cifrado de archivos (EFS)		EFS	Manual		
Sistema de eventos COM+		EventSystem	Automático		
SMP de Espacios de almacenamiento de Microsoft		smphost	Manual		
Solicitante de instantáneas de volumen de Hyper-V		vmicvss	Manual		
Superfetch		SysMain	Manual		
Tarjeta inteligente		SCardSvr	Deshabilitado		
Telefonía		TapiSrv	Deshabilitado		
Telemetría y experiencias del usuario conectado		DiagTrack	Automático		
Temas		Themes	Deshabilitado		
Ubicador de llamada a procedimiento remoto (RPC)		RpcLocator	Manual		
WalletService		WalletService	Manual		
Windows Driver Foundation - User-mode Driver Framework		wudfsvc	Manual		
Windows Installer		msiserver	Manual		
Windows Search		WSearch	Deshabilitado		
Windows Update		wuauserv	Manual		
12. Verifique los valores del registro.		Compruebe los valores del registro mediante el uso del “Editor del Registro”. **“Windows+R → Regedit”** 			

Comprobación	OK/NOK	Cómo hacerlo
		El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" para continuar. 

Directiva	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\NtfsDisable8dot3 NameCreation	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\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ ScreenSaverGracePeriod	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	

Comprobación	OK/NOK	Cómo hacerlo		
Directiva			**Valor**	**OK/NOK**
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\ TcpMaxDataRetransmissions			3	
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\ TCPMaxPortsExhausted			5	
13. Verifique los permisos asignados a ficheros y carpetas		Abra una ventana de Windows Explorer y diríjase a cada una de las rutas que indica el listado. Haga clic derecho con el ratón y seleccione “Propiedades” del menú.  **Nota**: Deberá tener cuidado para no realizar cambios sobre los permisos. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar". En la pestaña “Seguridad”, seleccione “Opciones Avanzadas”. 				

Comprobación	OK/NOK	Cómo hacerlo
		En la pantalla resultante, compruebe los permisos asignados a cada carpeta o fichero.  **Nota:** Deberá tener cuidado para no realizar cambios sobre los permisos. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar". Al pulsar sobre opciones avanzadas, en la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios al pulsar sobre el botón “Continuar”. Pulse “Sí” para ver los permisos. 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.

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\Registration	Administradores	Control total	
	System	Control total	
	Usuario	Leer y ejecución	
SystemRoot%\system32\cacls.exe	Administradores	Control total	
	System	Control total	
%SystemRoot%\system32\clip.exe	Administradores	Control total	
	System	Control total	
%SystemRoot%\system32\rasadhlp.dll	Administradores	Control total	
%SystemRoot%\system32\rasauto.dll	Administradores	Control total	
%SystemRoot%\system32\rasautou.exe	Administradores	Control total	
%SystemRoot%\system32\raschap.dll	Administradores	Control total	
%SystemRoot%\system32\rasctrnm.h	Administradores	Control total	
%SystemRoot%\system32\rasctrs.dll	Administradores	Control total	

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		**Usuario**	**Permiso**	**OK/NOK**
%SystemRoot%\system32\rasdial.exe		Administradores	Control total	
%SystemRoot%\system32\rasmans.dll		Administradores	Control total	
%SystemRoot%\system32\rasmontr.dll		Administradores	Control total	
%SystemRoot%\system32\rasphone.exe		Administradores	Control total	
%SystemRoot%\system32\rasppp.dll		Administradores	Control total	
%SystemRoot%\system32\rastapi.dll		Administradores	Control total	
%SystemRoot%\system32\runonce.exe		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\secedit.exe		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\tracert.exe		Administradores	Control total	
		System	Control total	

ANEXO A.3. CATEGORÍA MEDIA

ANEXO A.3.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE WINDOWS SERVER 2016 COMO SERVIDOR INDEPENDIENTE PARA LA CATEGORIA MEDIA

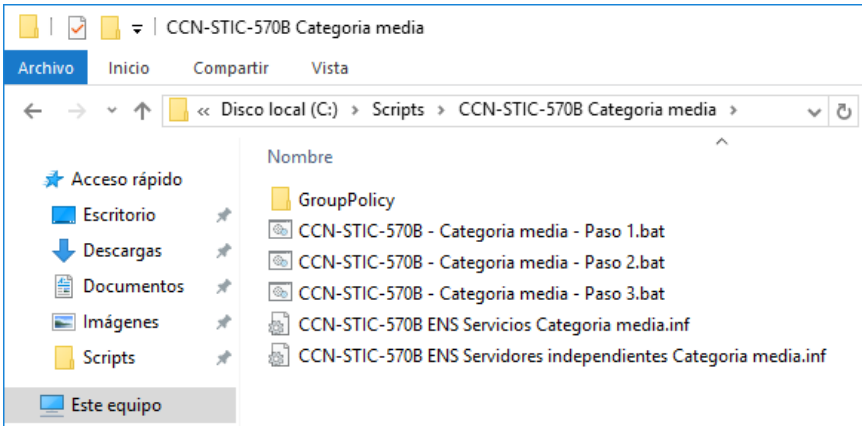
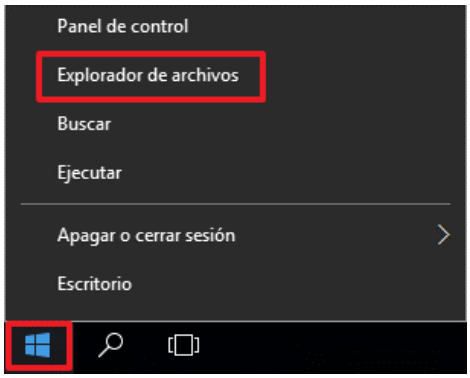
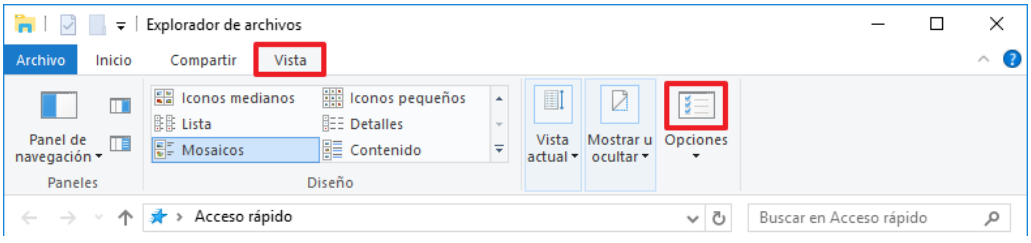
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se emplee Windows Server 2016, con una categorización de seguridad media, según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación 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, correspondiera a la categoría media, deberá realizar las implementaciones según se referencian en el presente anexo.

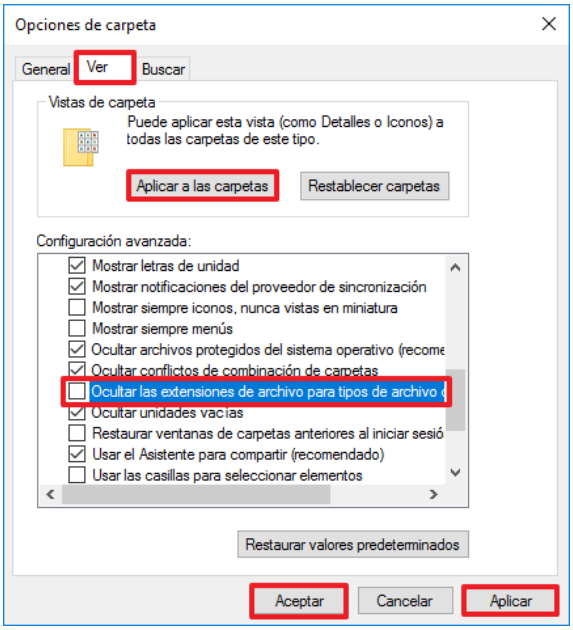
Se debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, será necesaria la realización de pruebas, en un entorno de preproducción, con objeto de familiarizarse con el escenario y comprobar la funcionalidad.

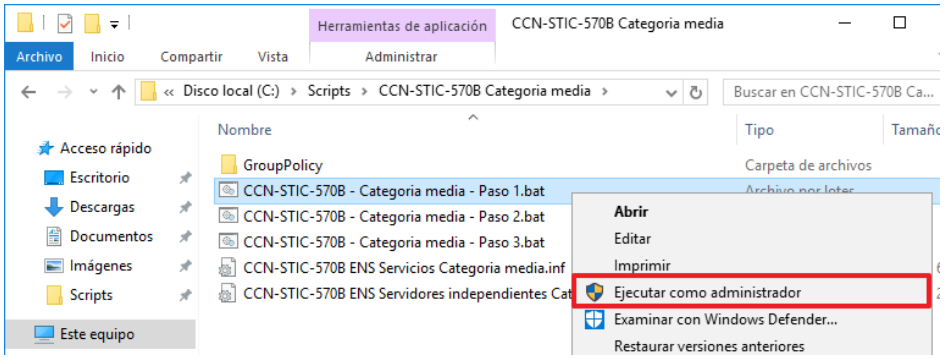
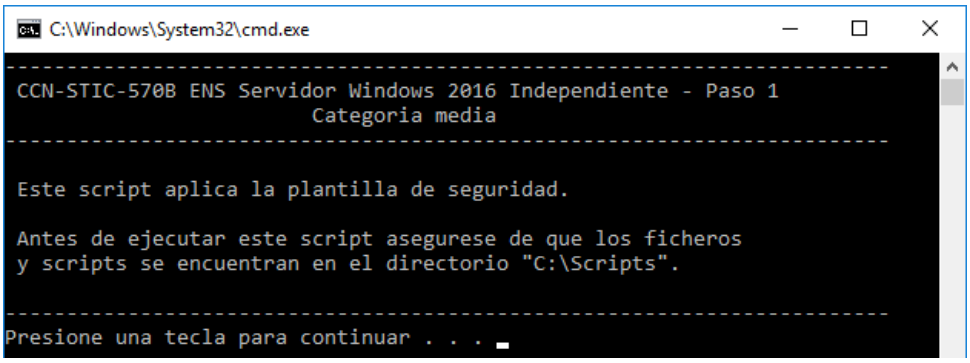
1. CONFIGURACIÓN DE LA SEGURIDAD LOCAL

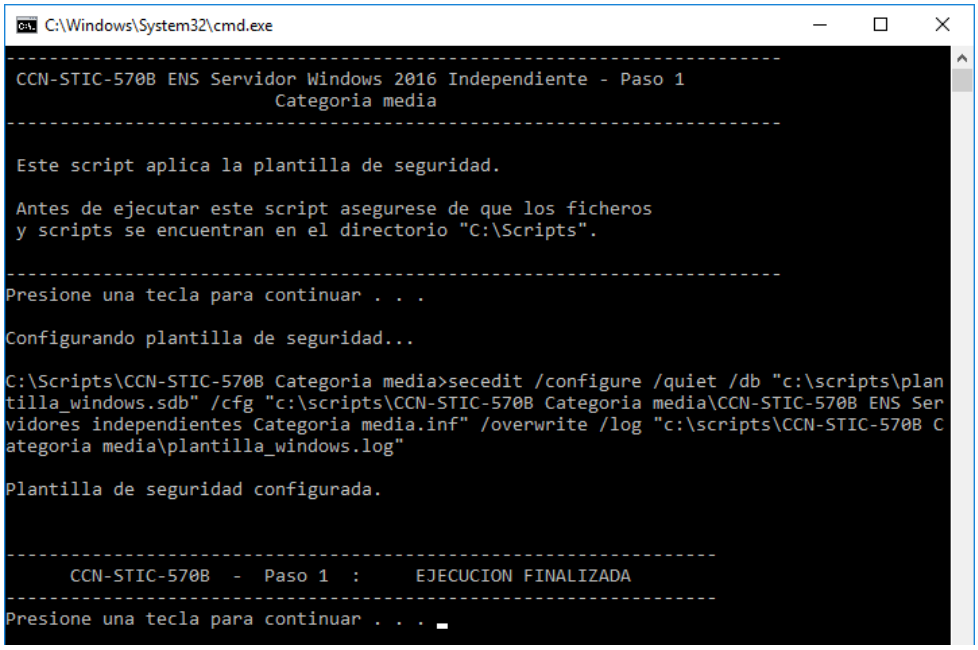
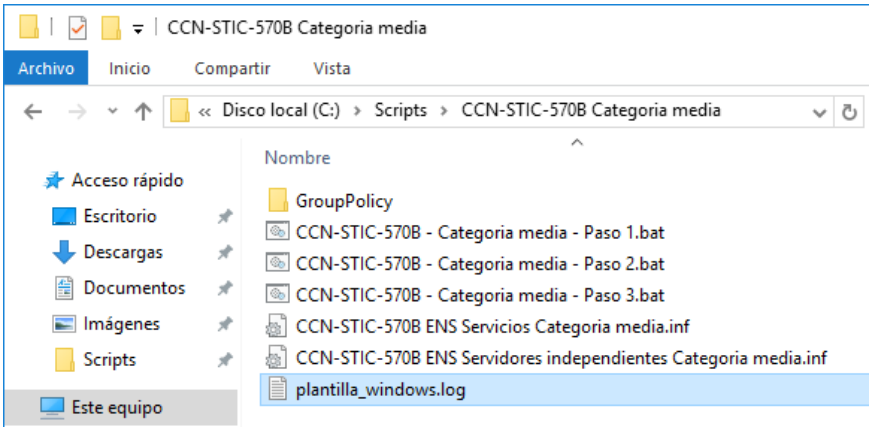
Los pasos que se describen a continuación se realizarán en todos aquellos servidores Windows Server 2016, independientes a un dominio, que implementen servicios o información de categoría media y que se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

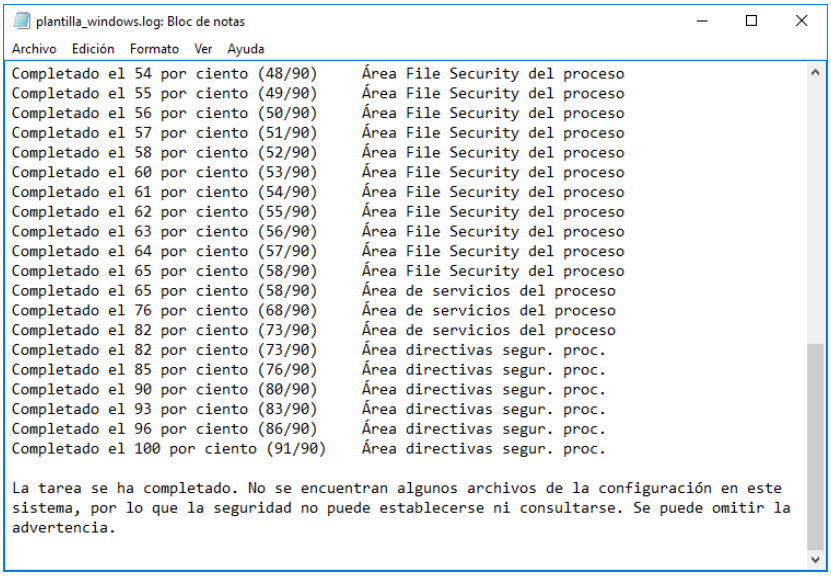
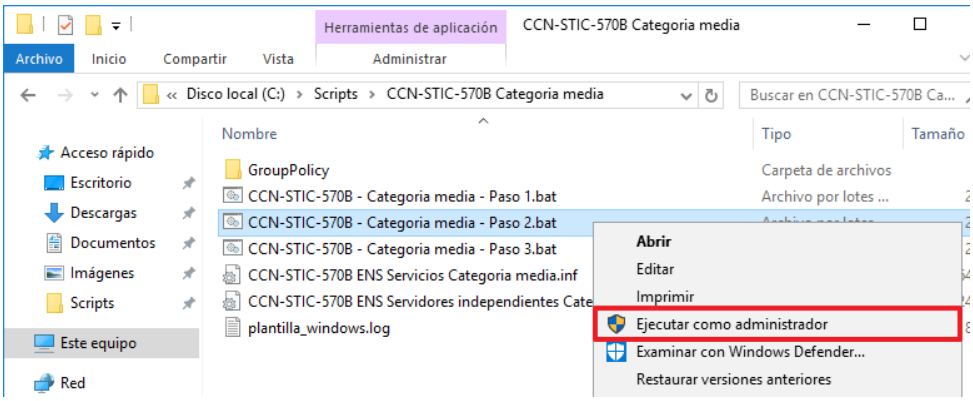
Paso	Descripción
1.	Inicie sesión en el servidor independiente donde se va aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del servidor.
3.	Cree el directorio “Scripts” en la unidad “C:\”.
4.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.

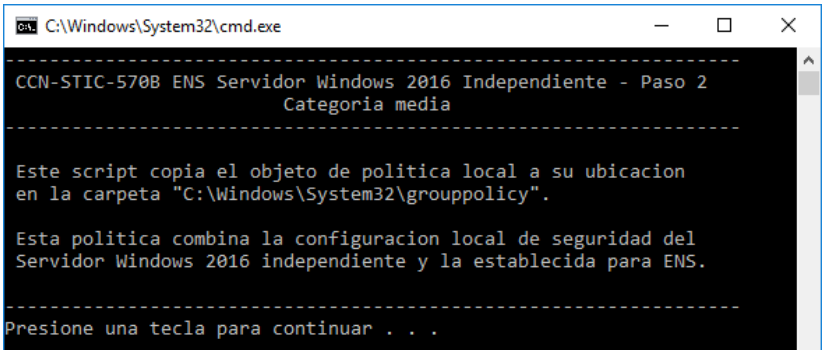
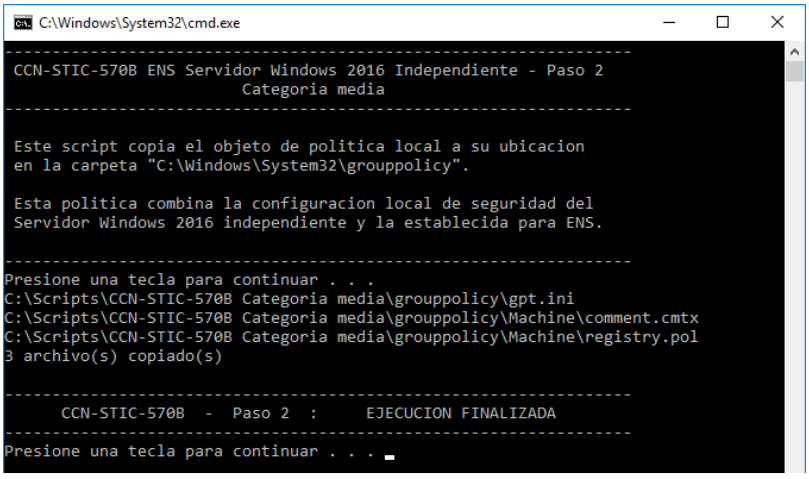
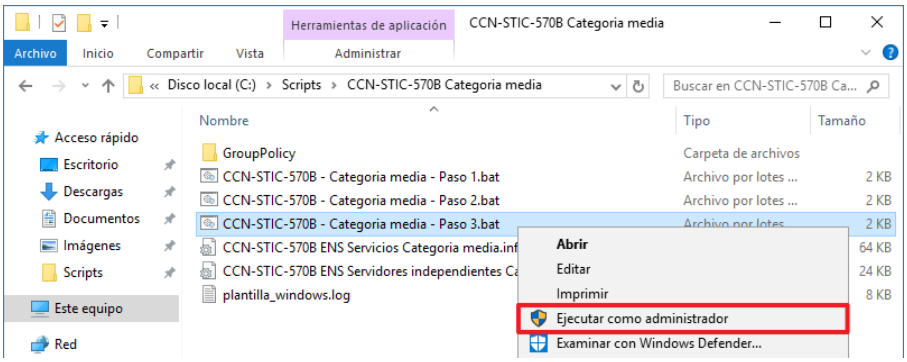
Paso	Descripción
5.	Abra la carpeta “CCN-STIC-570B Categoria media” que encontrará en la carpeta “C:\Scripts” que ha copiado. 
6.	Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de “Inicio” con el botón derecho y seleccione “Explorador de archivos”. 
7.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”. 

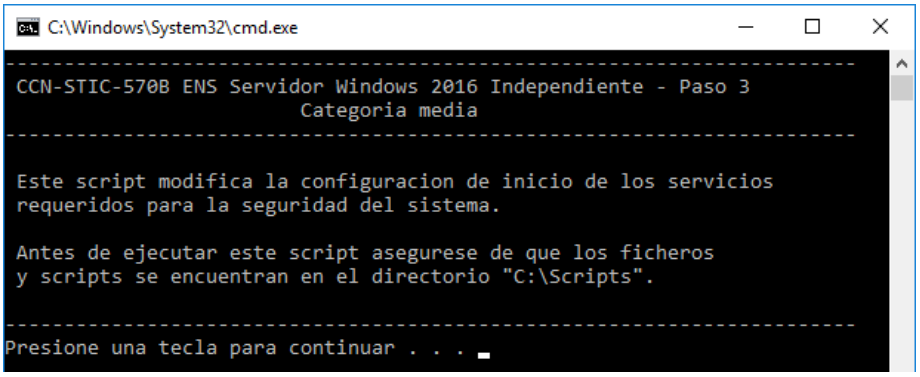
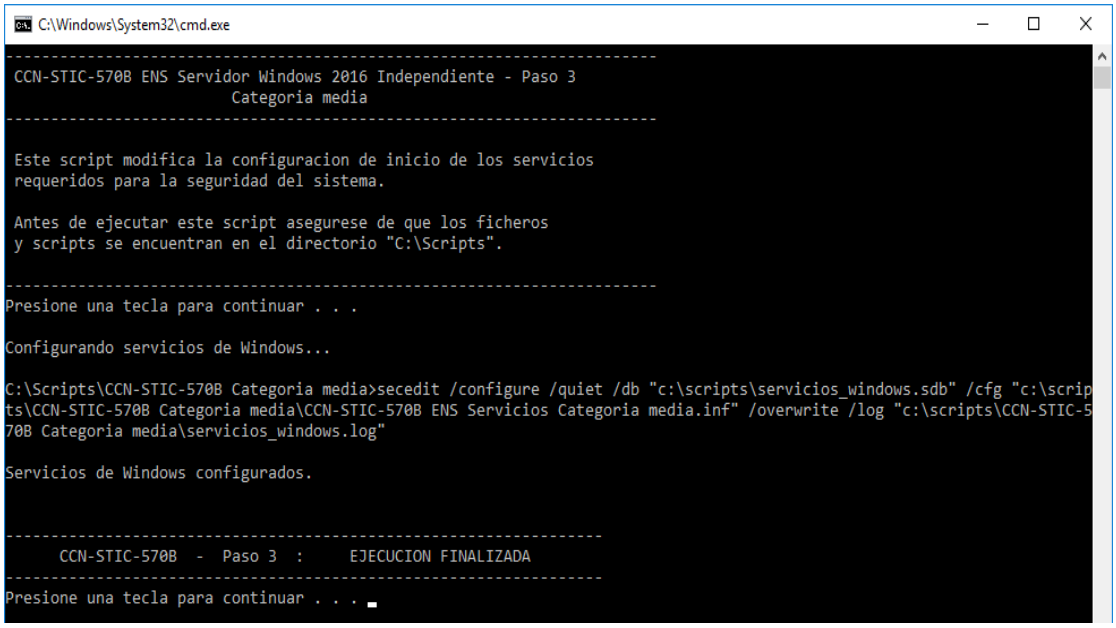
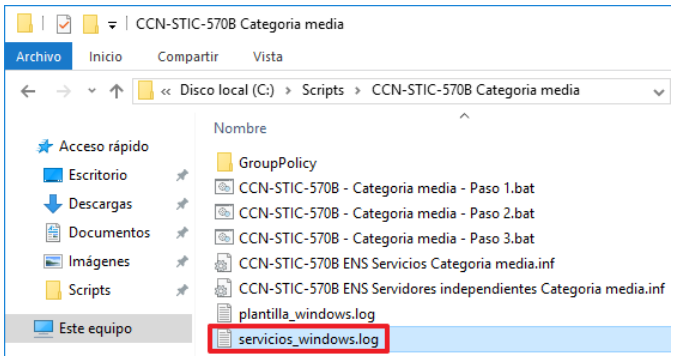
Paso	Descripción
8.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 
9.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio. – GroupPolicy (directorio) – CCN-STIC-570A Categoria Media – Paso 1.bat – CCN-STIC-570A Categoria Media – Paso 2.bat – CCN-STIC-570A Categoria Media – Paso 3.bat – CCN-STIC-570A ENS Servicios categoria media.inf – CCN-STIC-570A ENS Servidores independientes categoria media.inf

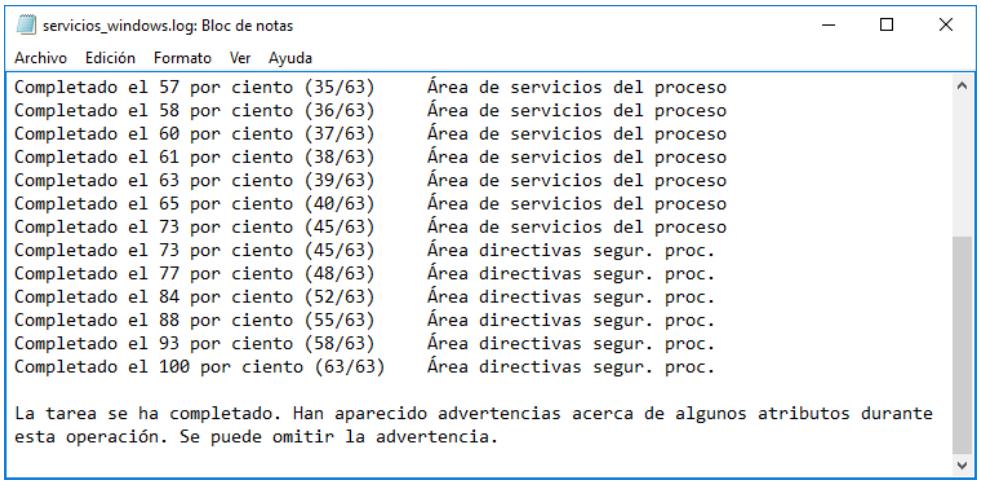
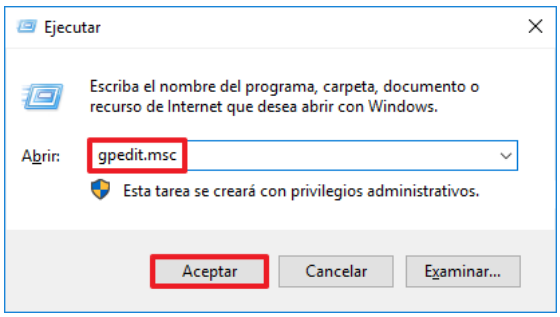
Paso	Descripción
10.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-570B – Categoria Media – Paso 1.bat” y seleccione la opción “Ejecutar como administrador”.  **Nota:** En función del usuario administrador con el que haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que le solicite elevación de privilegios, introducir credenciales de la cuenta del usuario con los privilegios de administrador o bien eleve automáticamente los privilegios sin solicitarle nada.
11.	Pulse una tecla para iniciar la ejecución del script que configurará la plantilla de seguridad con la seguridad requerida para la categoría media del ENS. 

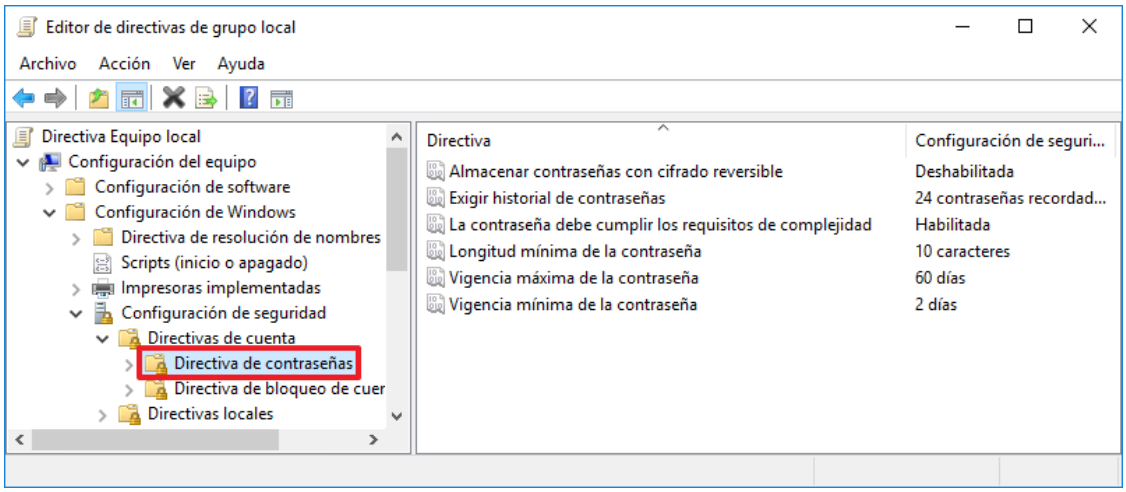
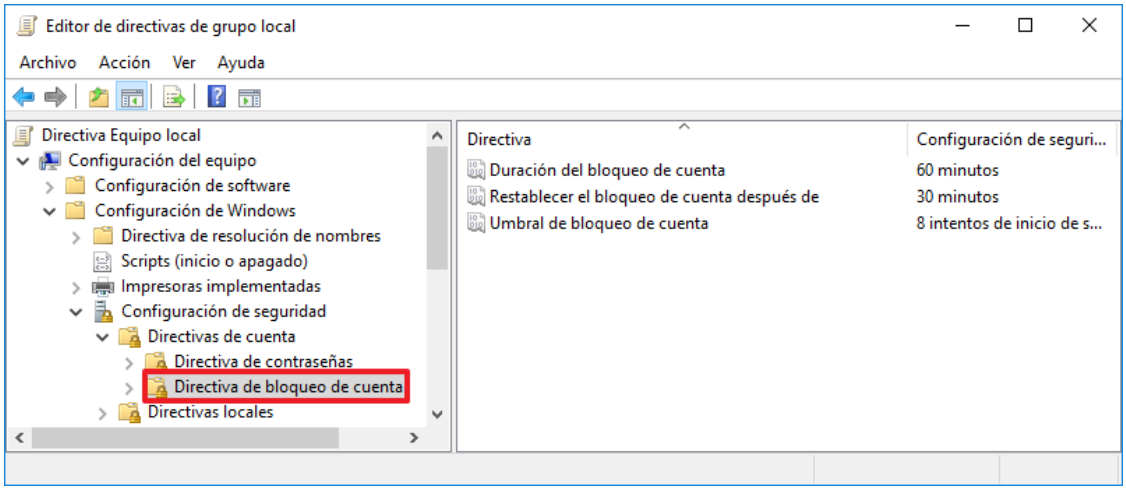
Paso	Descripción
12.	Una vez completado el proceso, deberá pulsar una tecla para continuar. 
13.	Pulse de nuevo otra tecla, para finalizar la ejecución del script. La ejecución del script genera un registro en la carpeta “C:\Scripts\CCN-STIC-570B Categoria media” con el nombre de “plantilla_windows.log”. 

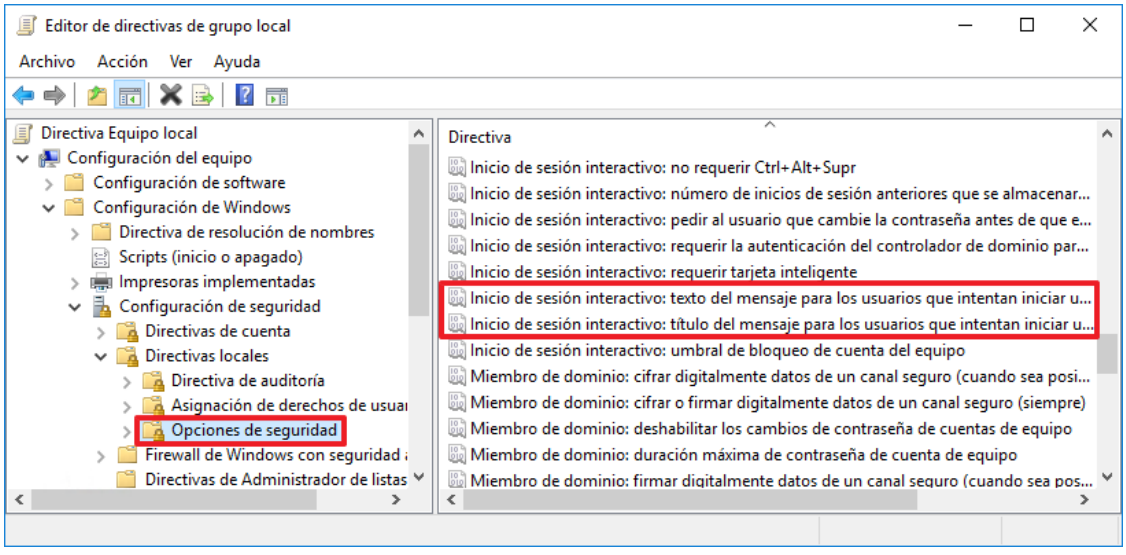
Paso	Descripción
14.	Abra este registro para comprobar si la configuración de la plantilla ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  **Nota:** En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script desde el paso 10.
15.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-570B – Categoria Media – Paso 2.bat” y seleccione la opción “Ejecutar como administrador”.  **Nota:** En función del usuario administrador con el que haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que le solicite elevación de privilegios, introducir credenciales de la cuenta del usuario con los privilegios de administrador o bien eleve automáticamente los privilegios sin solicitarle nada.

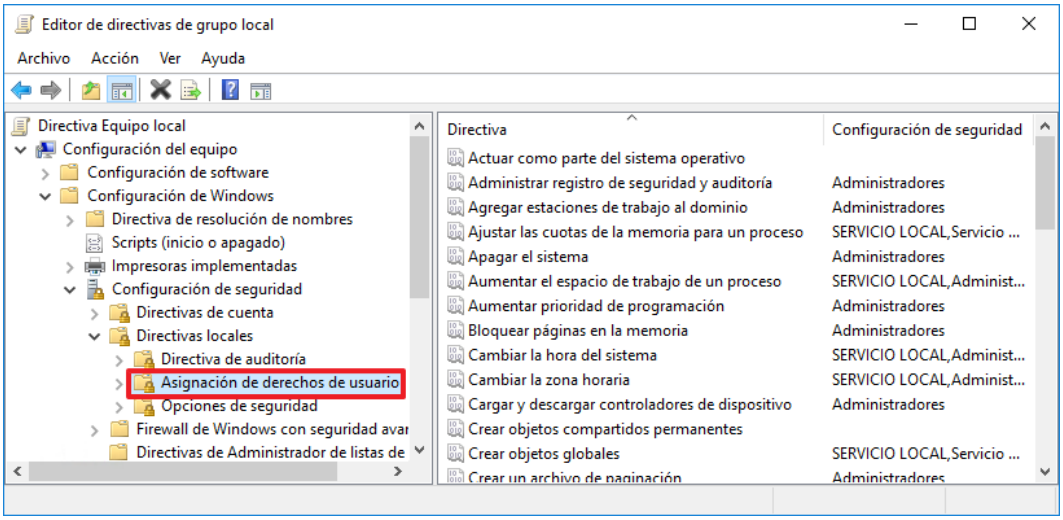
Paso	Descripción
16.	Pulse una tecla para iniciar la ejecución del script que configurará las plantillas administrativas con la seguridad requerida para la categoría media del ENS. 
17.	Una vez completado el proceso, deberá pulsar una tecla para continuar. 
18.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-570B – Categoria Media – Paso 3.bat” y seleccione la opción “Ejecutar como administrador”.  **Nota:** En función del usuario administrador con el que haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que le solicite elevación de privilegios, introducir credenciales de la cuenta del usuario con los privilegios de administrador o bien eleve automáticamente los privilegios sin solicitarle nada.

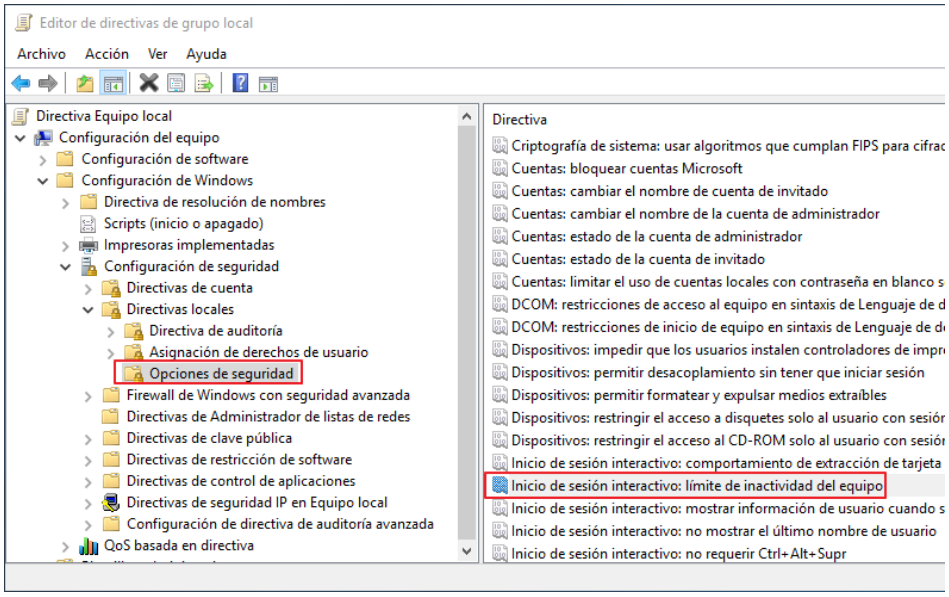
Paso	Descripción
19.	Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la categoría media del ENS. 
20.	Una vez completado el proceso, deberá pulsar una tecla para continuar. 
21.	Pulse de nuevo otra tecla, para finalizar la ejecución del script. La ejecución del script genera un registro en la carpeta “C:\Scripts\CCN-STIC-570B Categoria media con el nombre de “servicios_windows.log”. 

Paso	Descripción
22.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  **Nota:** En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script desde el paso 18.
23.	Es factible que su organización cuente con una política de contraseña consolidada. La implementación de la política de categoría media implementará una específica para los servidores con categoría media. Deberá evaluarla para determinar si esta configuración le es válida o por el contrario debe adaptarla a las condiciones de su organización.
24.	Inicie el “Editor de directivas de grupo local”. Para ello, vaya al menú “Ejecutar” y escriba “gpedit.msc” y pulse “Aceptar”. **“Tecla Windows + R → gpedit.msc”** 

Paso	Descripción
25.	Despliegue la política y sitúese en la siguiente ruta. **"Directiva Equipo Local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseña"** 
26.	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.
27.	De forma similar a lo anterior, deberá evaluar la política de bloqueo de cuenta. Para ello y sin cerrar el editor, seleccione la "Directiva de bloqueo de cuenta" que encontrará al mismo nivel que la directiva de contraseñas. 
28.	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.

Paso	Descripción
29.	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.
30.	Para informar de las obligaciones sitúese en la siguiente ruta. **"Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"**
31.	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". 
32.	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.

Paso	Descripción
33.	Por último, la política de seguridad local especifica 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 haya asignado derechos determinados para la administración o gestión de los sistemas. Si esto fuera así deberá realizar las modificaciones sobre la configuración de política local.
34.	Despliegue la política y sitúese en la siguiente ruta. **"Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"** 
35.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
36.	Se establece a partir de la categoría media, según MP. EQ. 2 la necesidad de realizar el bloqueo del equipo ante un tiempo razonable de inactividad. A través de la política local aplicable sobre usuario, puede establecerse la medida de protección que habilita el salvapantallas y por lo tanto el bloqueo de la sesión. **Nota:** Si la organización presenta algún mecanismo 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
37.	Despliegue la política y sitúese en la siguiente ruta. **"Configuración de equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"** 
38.	Habilite y configure la siguiente directiva de seguridad. – Inicio de sesión interactivo: límite de actividad del equipo – Establezca el valor en 600 segundos (10 minutos).
39.	Cierre el "Editor de directivas de grupo local".
40.	Elimine la carpeta "C:\Scripts" y su contenido.
41.	Reinicie el servidor.

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

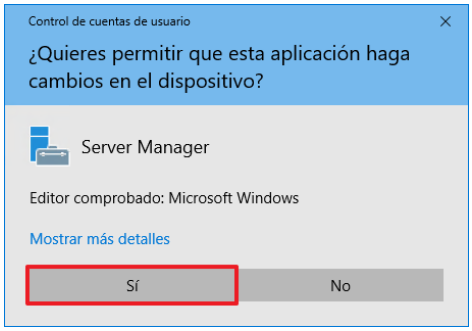
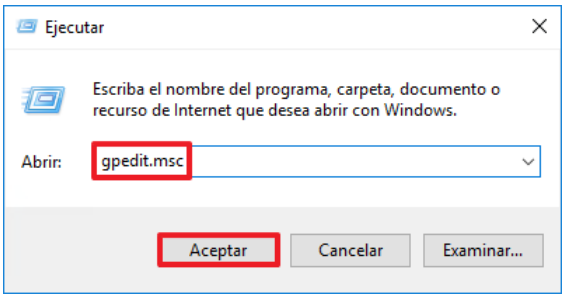
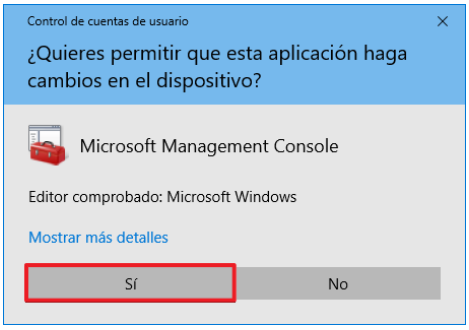
El control de cuentas de usuario surge, en Windows Vista, como respuesta para limitar las acciones de los administradores cuando actuaban con cuentas privilegiadas ante operativas que no requerían dicho privilegio. En sistemas previos a Windows Vista, un administrador que había iniciado una sesión actuaba 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.

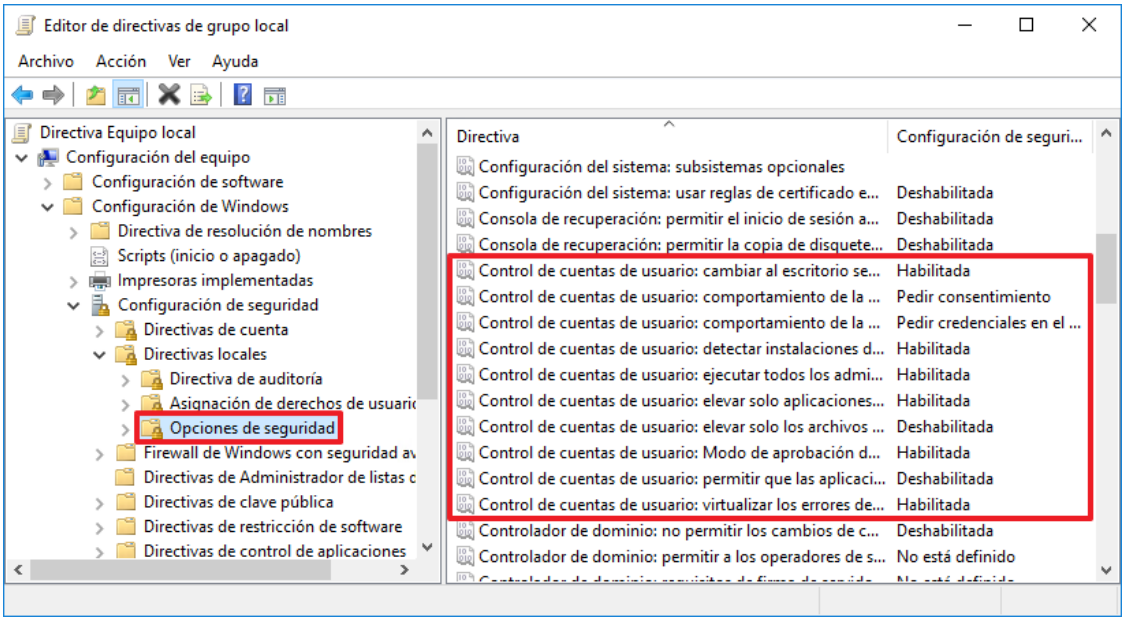
Siguiendo el principio de menor privilegio y menor exposición, la presente guía habilita las condiciones de funcionalidad de UAC para la categoría media, aunque con los criterios más laxos de los aplicables.

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 modificación de la política local, de seguridad de aplicación a los servidores miembros, que pudieran presentar incidencias con la configuración de UAC.

Debe tenerse en cuenta 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.

Paso	Descripción
42.	Inicie sesión en el servidor independiente con una cuenta de administrador local. El sistema le solicitará elevación de privilegios para poder ejecutar la herramienta "Administrador del servidor". Pulse "Sí" para continuar. 
43.	Inicie el "Editor de directivas de grupo local". Para ello, vaya al menú "Ejecutar" y escriba "gpedit.msc" y pulse "Aceptar". **"Tecla Windows + R → gpedit.msc"** 
44.	Pulse "Sí" cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 

Paso	Descripción
45.	Despliegue la política local y sitúese en la siguiente ruta. **"Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"**
46.	Identifique las directivas relativas a "Control de cuenta de usuario". 
47.	Realice las modificaciones oportunas.
48.	Cierre la política.
49.	Reinicie el servidor. **Nota:** Debe tener en consideración que, si ha alterado la política de control de cuentas y ésta es menos rigurosa que la propuesta en la configuración deseada de 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.3.2. LISTA DE COMPROBACIÓN DE WINDOWS SERVER 2016 COMO SERVIDOR INDEPENDIENTE 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.3.1 PASO A PASO DE IMPLEMENTACIÓN SEGURA DE WINDOWS SERVER 2016 COMO SERVIDOR INDEPENDIENTE PARA LA A".

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

Para realizar esta lista de comprobación deberá iniciar sesión en el servidor con una cuenta de usuario que tenga privilegios de administrador local.

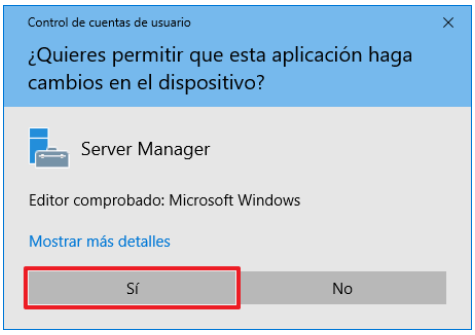
Para realizar las comprobaciones pertinentes en el servidor se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local. Las consolas y herramientas que se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

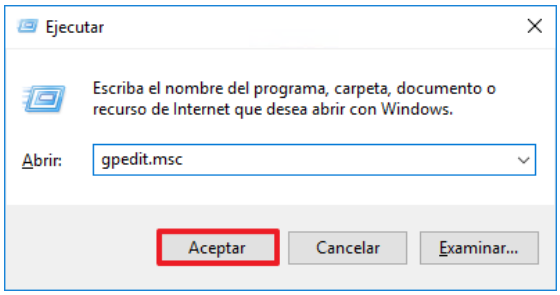
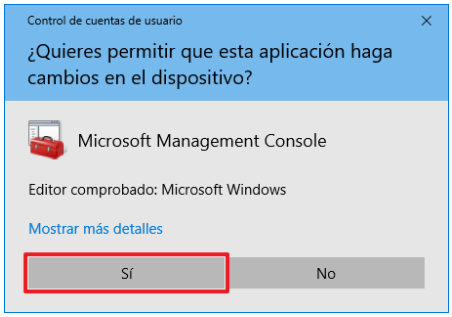
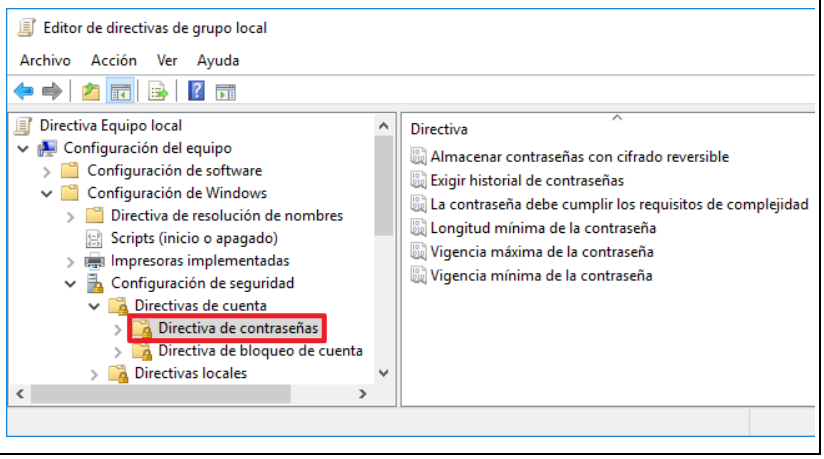
a) Editor de objetos de directiva de grupo local (gpedit.msc)

b) Editor de registro (regedit.exe)

c) Visor de Eventos (eventvwr.exe)

d) Servicios (services.msc)

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el servidor.		Inicie sesión en el servidor independiente con una cuenta de administrador local. El sistema le solicitará elevación de privilegios para poder ejecutar la herramienta "Administrador del servidor. Pulse "Sí" para continuar. 

Comprobación	OK/NOK	Cómo hacerlo
2. Verifique la directiva de contraseñas en el editor de objetos de directiva de grupo local.		Inicie el "Editor de directivas de grupo local". Para ello, vaya al menú ejecutar y escriba "gpedit.msc" y pulse "Aceptar". **"Tecla Windows + R → gpedit.msc"**  Pulse "Sí" cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo.  En el "Editor de objetos de directiva de grupo local" seleccione el siguiente nodo: **"Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de contraseñas"** 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="7"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Almacenar contraseñas usando cifrado reversible</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Exigir historial de contraseñas</td><td>24 contraseñas recordadas</td><td></td></tr>
<tr><td colspan="2">Las contraseñas deben cumplir los requisitos de complejidad</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Longitud mínima de la contraseña</td><td>10 caracteres</td><td></td></tr>
<tr><td colspan="2">Vigencia máxima de la contraseña</td><td>60 días</td><td></td></tr>
<tr><td colspan="2">Vigencia mínima de la contraseña</td><td>2 días</td><td></td></tr>
<tr><td rowspan="5">3. Verifique las directivas de bloqueo de cuenta en el editor de objetos de directiva de grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo local → Configuración del Equipo → 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>60 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="8">4. Verifique las directivas de auditoría en el editor de objetos de directiva de grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”</td></tr>
<tr><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>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="4"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">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="19">5. Verifique la asignación de derechos de usuario en el editor de objetos de directiva de grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → 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>
<tr><td colspan="2">Cambiar la zona horaria</td><td>SERVICIO LOCAL, Administradores</td><td></td></tr>
<tr><td colspan="2">Cargar y descargar controladores de dispositivo</td><td>Administradores</td><td></td></tr>
<tr><td colspan="2">Crear objetos globales</td><td>Administradores, SERVICIO, SERVICIO LOCAL, Servicio de red</td><td></td></tr>
<tr><td colspan="2">Crear un archivo de paginación</td><td>Administradores</td><td></td></tr>
<tr><td colspan="2">Crear vínculos simbólicos</td><td>Administradores</td><td></td></tr>
<tr><td colspan="2">Denegar el acceso a este equipo desde la red</td><td>ANONYMOUS LOGON, Invitados</td><td></td></tr>
<tr><td colspan="2">Denegar el inicio de sesión como servicio</td><td>Invitados</td><td></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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 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	
		Omitir comprobación de recorrido	Todos, SERVICIO LOCAL, Servicio de red, Administradores, Usuarios, Operadores de copia de seguridad.	
		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	

<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">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>6. Verifique las opciones de seguridad en el editor de objetos de directiva de grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:

“Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”</td></tr>
</table>

Directiva	Valor	OK/NOK
Acceso a redes: modelo de seguridad y uso compartido para cuentas locales	Clásico: usuarios locales se autentican con credenciales propias	
Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red	Habilitada	
Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Habilitada	
Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Habilitada	
Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	Deshabilitada	
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	

Comprobación	OK/NOK	Cómo hacerlo

Directiva	Valor	OK/NOK
Acceso a redes: rutas y subrutas del registro accesibles remotamente	System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\EventLog Software\Microsoft\OLAP Server Software\Microsoft\WindowsNT\CurrentVersion\Print Software\Microsoft\WindowsNT\CurrentVersion\Windows System\CurrentControlSet\Control\Content Index System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\Currente Version\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	
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	Deshabilitada	
Auditoría: auditar el uso del privilegio de copias de seguridad y restauración	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	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		**Valor**	**OK/NOK**
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)		Habilitada	
Configuración del sistema: Usar reglas de certificado en ejecutables de Windows para directivas de restricción de software		Deshabilitada	
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	
Control de cuentas de usuario: elevar solo aplicaciones UIAccess instaladas en ubicaciones seguras		Habilitada	
Control de cuentas de usuario: elevar solo los archivos ejecutables firmados y validados		Deshabilitada	
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	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		**Valor**	**OK/NOK**
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 del 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	
Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash		Deshabilitada	
Cuentas: cambiar el nombre de cuenta de invitado		Invitado	
Cuentas: cambiar el nombre de cuenta administrador		Administrador	
Cuentas: estado de la cuenta de administrador		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;;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	
Dispositivos: restringir el acceso a disquetes sólo al usuario con sesión iniciada localmente		Habilitada	
Dispositivos: restringir el acceso a CD-ROM sólo al usuario con sesión iniciada localmente		Habilitada	

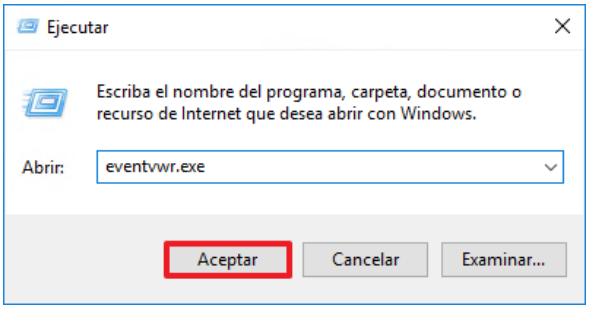
Comprobación	OK/NOK	Cómo hacerlo	
Directiva		**Valor**	**OK/NOK**
Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente		Bloquear estación de trabajo	
Inicio de sesión interactivo: mostrar información de usuario cuando se bloquee la sesión		No mostrar información del usuario	
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	
Inicio de sesión interactivo: requerir tarjeta inteligente		Deshabilitada	
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	

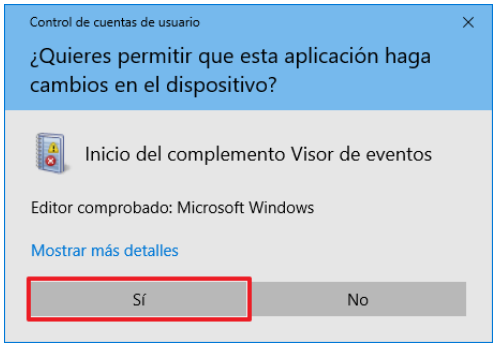
Comprobación	OK/NOK	Cómo hacerlo	
Directiva		**Valor**	**OK/NOK**
Objetos del sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que no sean de Windows		Habilitada	
Seguridad de red: configurar tipos de cifrado permitidos para Kerberos		RC4_HMAC_MD5, AES128_HMAC_SHA1, AES2656_HMAC_SHA1, Tipos de cifrados futuros	
Seguridad de red: forzar el cierre de sesión cuando expire la hora de sesión		Deshabilitada	
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	
Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)		Requerir cifrado de 128 bits	
Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)		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	

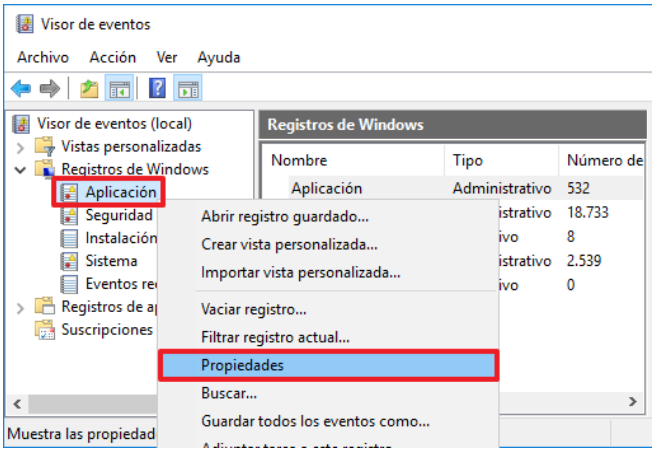
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td colspan="2">Directiva</td><td colspan="2">Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)</td><td colspan="2">Habilitada</td><td></td></tr>
<tr><td colspan="2">Servidor de red de Microsoft: nivel de validación de nombres de destino SPN del servidor</td><td colspan="2">Requerido del cliente</td><td></td></tr>
<tr><td colspan="2">Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión</td><td colspan="2">15 minutos</td><td></td></tr>
<tr><td rowspan="2">7. Verifique las directivas del almacén digital en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → Plantillas administrativas → Componentes de Windows → Administración de derechos digitales de Windows Media”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Impedir el acceso a Internet de Windows Media DRM</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="2">8. Verifique las directivas del almacén digital en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → Plantillas administrativas → 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>9. Verifique las directivas del informe de errores de Windows en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Biometría”</td></tr>
</table>

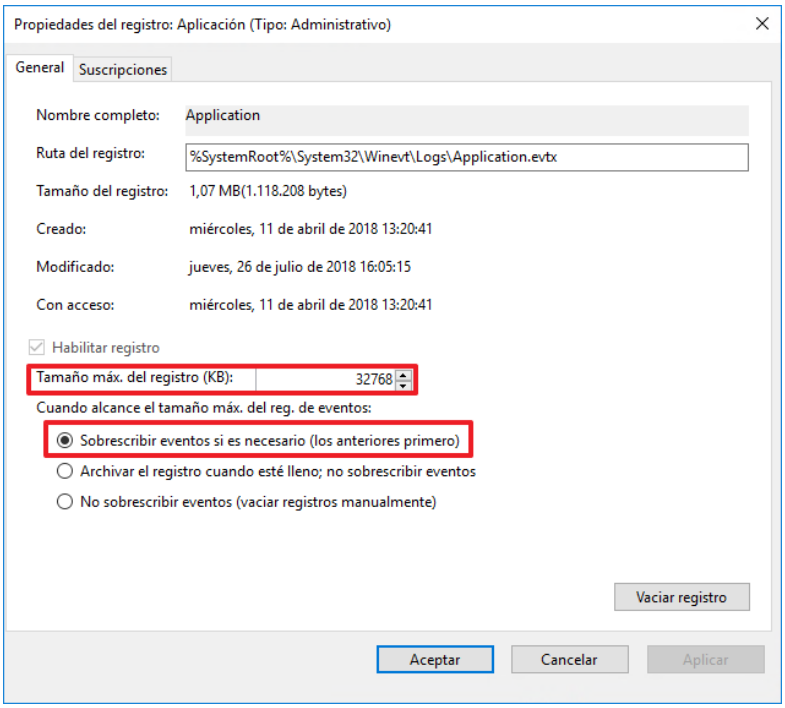
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="4"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Permitir el uso de biometría</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Permitir que los usuarios de dominio inicien sesión mediante biometría</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Permitir que los usuarios inicien sesión mediante biometría</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="4">10. Verifique las directivas del informe de errores de Windows en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Directivas de reproducción automática”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Establece el comportamiento predeterminado para la ejecución automática</td><td>Habilitado</td><td></td></tr>
<tr><td colspan="2">Desactivar reproducción automática</td><td>Habilitado</td><td></td></tr>
<tr><td rowspan="4">11. Verifique las directivas del informe de errores de Windows en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → Plantillas Administrativas → 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>12. Verifique las directivas del informe de errores de Windows en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Opciones de inicio de sesión de Windows”</td></tr>
</table>

<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">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>
<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 rowspan="3">13. Verifique las directivas del informe de errores de Windows en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Shell remoto de Windows”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Permitir acceso a Shell remoto</td><td>Deshabilitada</td><td></td></tr>
<tr><td rowspan="10">14. Verifique la configuración de la comunicación de Internet en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → Plantillas Administrativas → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Desactivar informe de errores de reconocimiento de escritura a mano</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar el Programa para la mejora de la experiencia de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar los vínculos “Events.asp” del Visor de eventos</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar el contenido “¿Sabía que…?” del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar la búsqueda en Microsoft Knowledge Base del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar el informe de errores de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar la actualización de archivos de contenido del Asistente para búsqueda</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar el acceso a la Tienda</td><td>Habilitada</td><td></td></tr>
</table>

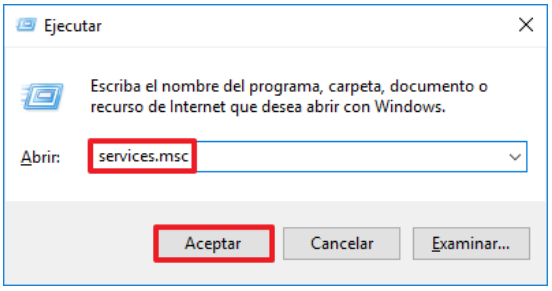
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="3"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Desactivar la tarea de imágenes “Pedir copias fotográficas”</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="3">15. Verifique las directivas del informe de errores de Windows en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → Plantillas Administrativas → Sistema → Net Logon”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Permitir algoritmos de criptografía compatibles con Windows NT 4.0</td><td>Deshabilitada</td><td></td></tr>
<tr><td>16. Verifique la configuración del registro de eventos en el editor de objetos de directiva de grupo local.</td><td></td><td colspan="3">Inicie el “Visor de eventos”. Para ello, vaya al menú ejecutar, escriba “eventvwr.exe” y pulse “Aceptar”.
“Tecla Windows + R →eventvwr.exe”
 

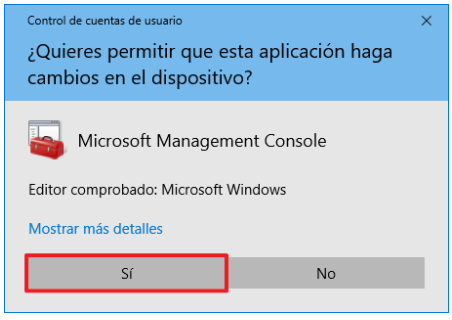
El “Control de cuentas de usuario” solicitará elevación de privilegios. Pulse “Sí” para continuar.
 
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>
En el “Visor de eventos” despliegue el contenedor “Registros de Windows” y seleccione propiedades haciendo clic derecho sobre “Aplicación”.




Repita el proceso para “Seguridad” y “Sistema”.
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Cuando alcance el tamaño máximo del registro de eventos de la aplicación</td><td>Sobrescribir eventos si es necesario (los anteriores primero)</td><td></td></tr>
<tr><td>Tamaño máximo del registro de la aplicación</td><td>32768 kilobytes</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="5"></td><td rowspan="5"></td><th colspan="2">Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td colspan="2">Cuando alcance el tamaño máximo del registro de eventos de seguridad</td><td>Sobrescribir eventos si es necesario (los anteriores primero)</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">Cuando alcance el tamaño máximo del registro de eventos del sistema</td><td>Sobrescribir eventos si es necesario (los anteriores primero)</td><td></td></tr>
<tr><td colspan="2">Tamaño máximo del registro del sistema</td><td>32768 kilobytes</td><td></td></tr>
<tr><td>17. Verifique el modo de configuración de los servicios del sistema</td><td></td><td colspan="4">Inicie la consola de “Servicios”. Para ello, vaya al menú ejecutar, escriba “services.msc” y pulse “Aceptar”.
“Tecla Windows + R →services.msc”
 

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

Nota: Dependiendo del equipo, es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales (antivirus, etc.).</td></tr>
</table>

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

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

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

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

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

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

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

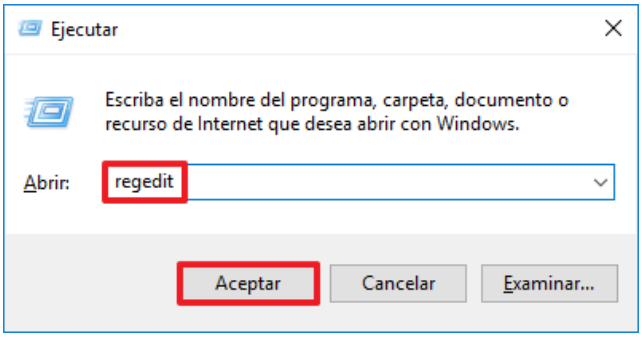
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de repositorio de estado	StateRepository	Manual		
Servicio de sensores	SensorService	Manual		
Servicio de servidor proxy KDC (KPS)	KPSSVC	Manual		
Servicio de sincronización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

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

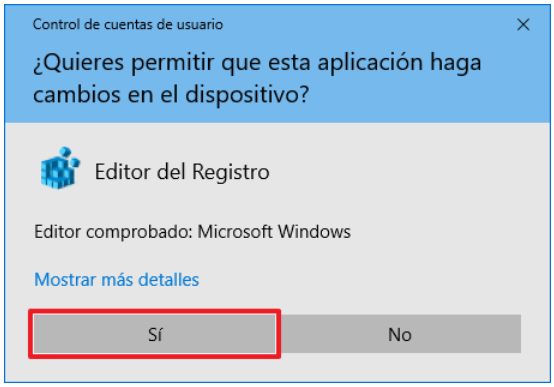
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Temas	Themes	Deshabilitado		
Ubicador de llamada a procedimiento remoto (RPC)	RpcLocator	Manual		
WalletService	WalletService	Manual		
Windows Driver Foundation - User-mode Driver Framework	wudfsvc	Manual		
Windows Installer	msiserver	Manual		
Windows Search	WSearch	Deshabilitado		
Windows Update	wuauserv	Manual		

18. Verifique los valores del registro.

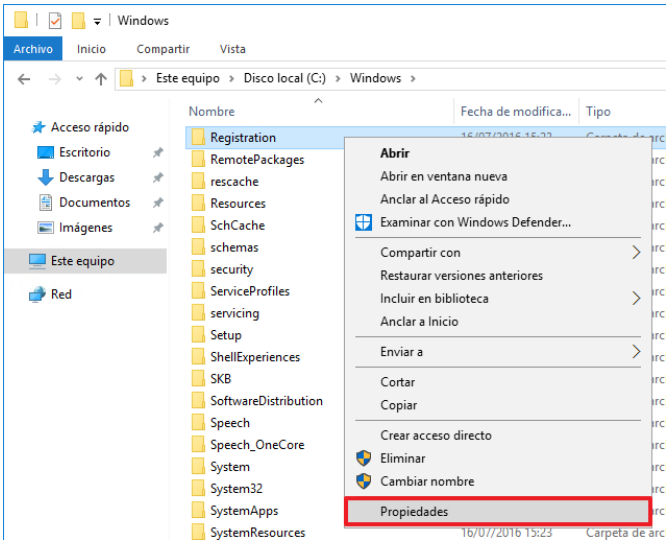
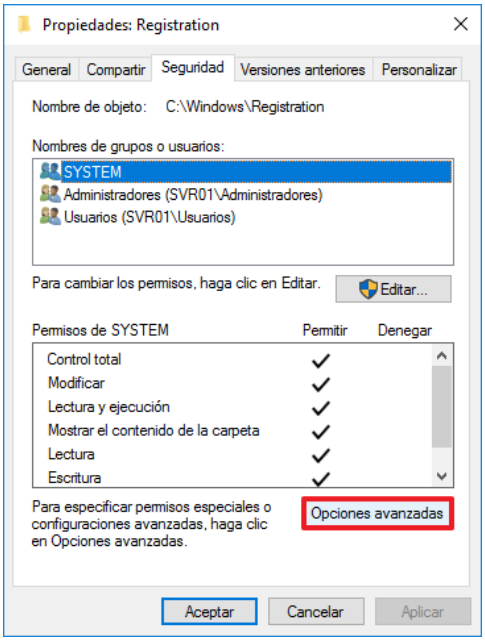
Compruebe los valores del registro mediante el uso del "Editor del Registro".
"Windows+R → Regedit"

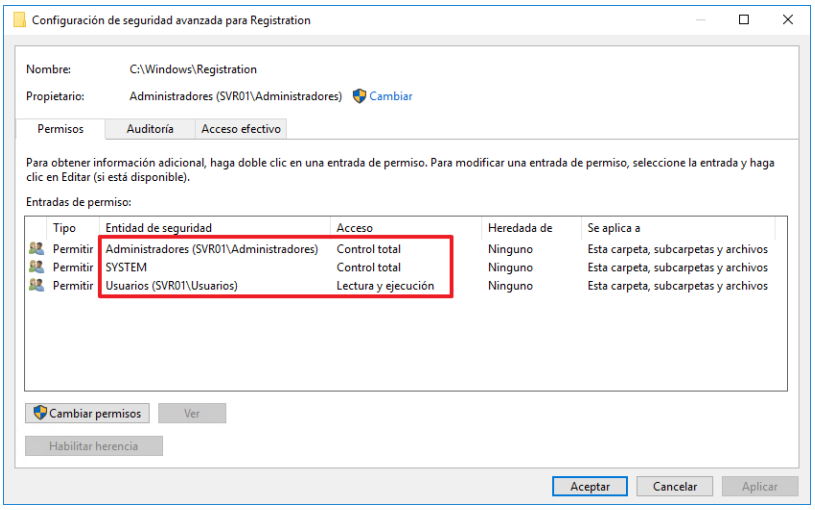


El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" para continuar.



Comprobación	OK/NOK	Cómo hacerlo	
Directiva		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\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ ScreenSaverGracePeriod		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	

Comprobación	OK/NOK	Cómo hacerlo
19. Verifique los permisos asignados a ficheros y carpetas		Abra una ventana de Windows Explorer y diríjase a cada una de las rutas que indica el listado. Haga clic derecho con el ratón y seleccione “Propiedades” del menú.  **Nota:** Deberá tener cuidado para no realizar cambios sobre los permisos. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar". En la pestaña “Seguridad”, seleccione “Opciones Avanzadas”. 

Comprobación	OK/NOK	Cómo hacerlo
		En la pantalla resultante, compruebe los permisos asignados a cada carpeta o fichero.  **Nota:** Deberá tener cuidado para no realizar cambios sobre los permisos. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar". Al pulsar sobre opciones avanzadas, en la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios al pulsar sobre el botón “Continuar”. Pulse “Sí” para ver los permisos. 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.

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\Registration	Administradores	Control total	
	System	Control total	
	Usuario	Leer y ejecución	
%SystemRoot%\system32\cacls.exe	Administradores	Control total	
	System	Control total	
%SystemRoot%\system32\clip.exe	Administradores	Control total	
	System	Control total	
%SystemRoot%\system32\rasadhlp.dll	Administradores	Control total	
%SystemRoot%\system32\rasauto.dll	Administradores	Control total	
%SystemRoot%\system32\rasautou.exe	Administradores	Control total	
%SystemRoot%\system32\raschap.dll	Administradores	Control total	
%SystemRoot%\system32\rasctrnm.h	Administradores	Control total	

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		**Usuario**	**Permiso**	**OK/NOK**
%SystemRoot%\system32\rasctrs.dll		Administradores	Control total	
%SystemRoot%\system32\rasdial.exe		Administradores	Control total	
%SystemRoot%\system32\rasmans.dll		Administradores	Control total	
%SystemRoot%\system32\rasmontr.dll		Administradores	Control total	
%SystemRoot%\system32\rasphone.exe		Administradores	Control total	
%SystemRoot%\system32\rasppp.dll		Administradores	Control total	
%SystemRoot%\system32\rastapi.dll		Administradores	Control total	
%SystemRoot%\system32\runonce.exe		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\secedit.exe		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\tracert.exe		Administradores	Control total	
		System	Control total	

ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.4.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE WINDOWS SERVER 2016 COMO SERVIDOR INDEPENDIENTE PARA LA CATEGORÍA ALTA

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.

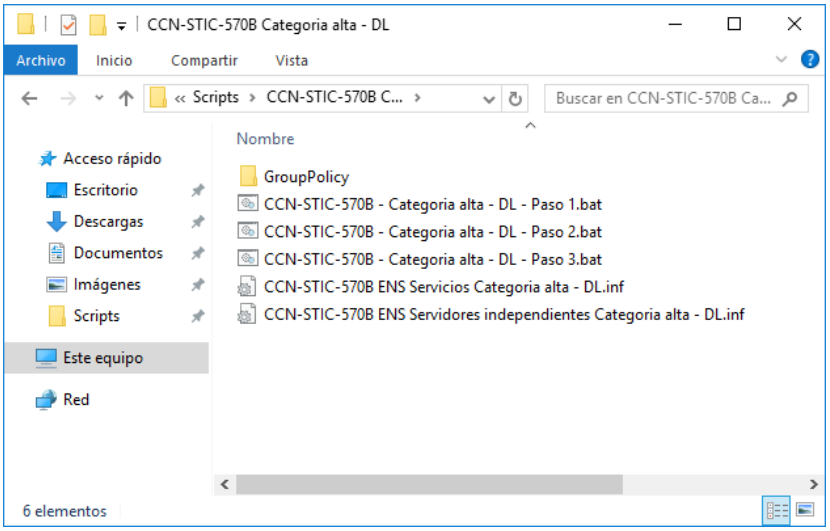
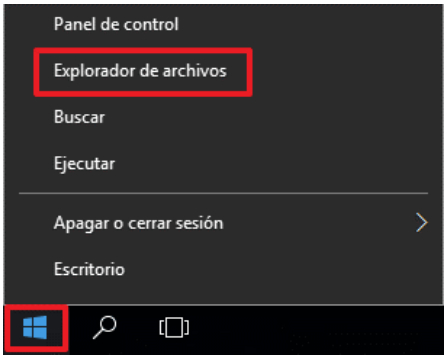
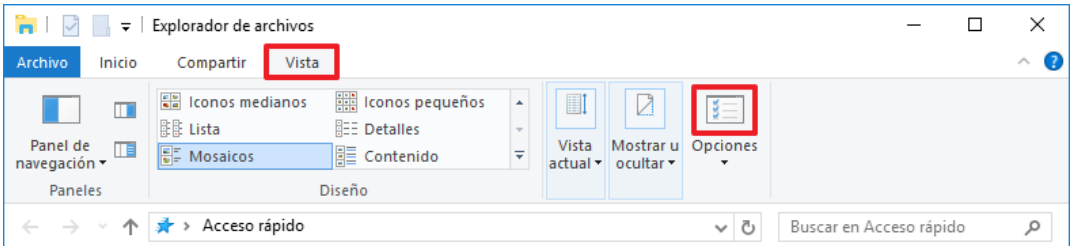
Nota: Tenga en cuenta que en el caso de una red clasificada con grado de clasificación Difusión Limitada se hará usó de la aplicación de seguridad descrita en este anexo, pero deberá atender adicionalmente a los requisitos establecidos por la normativa de aplicación sobre sistemas clasificados para dicho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

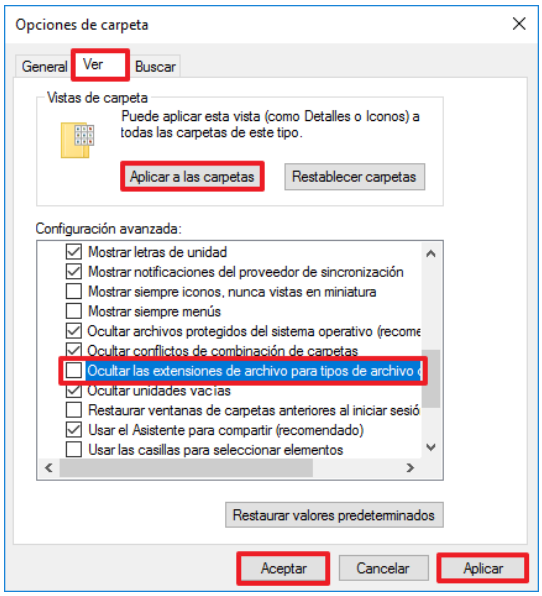
Se debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, será necesaria la realización de pruebas, en un entorno de preproducción, con objeto de familiarizarse con el escenario y comprobar la funcionalidad.

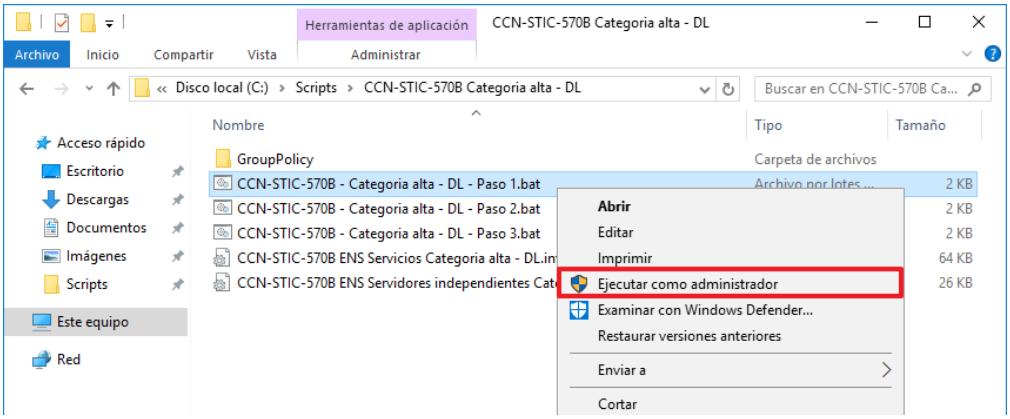
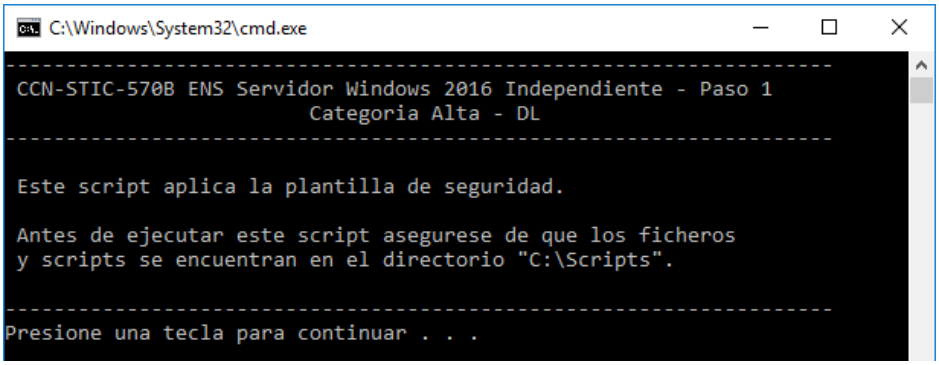
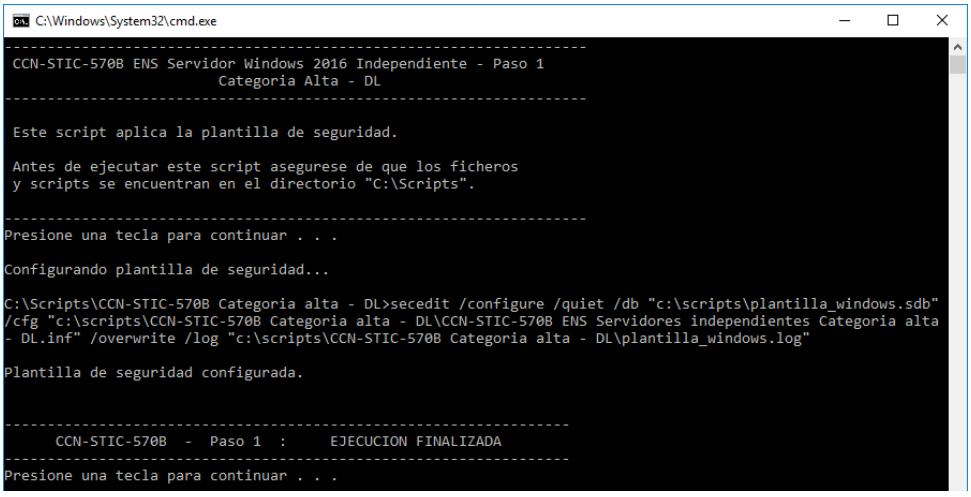
1. CONFIGURACIÓN DE LA SEGURIDAD LOCAL

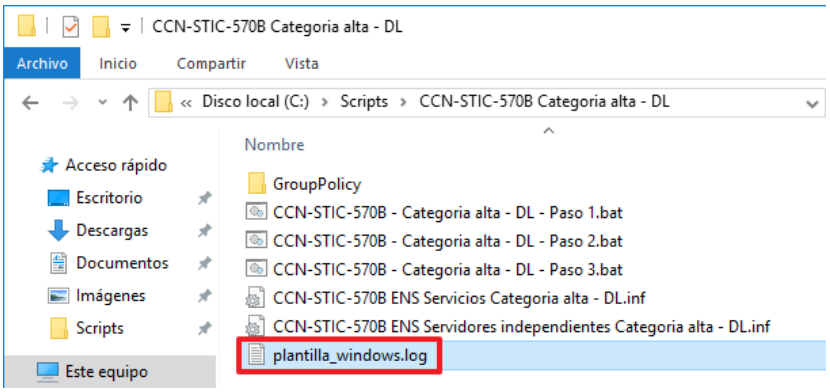
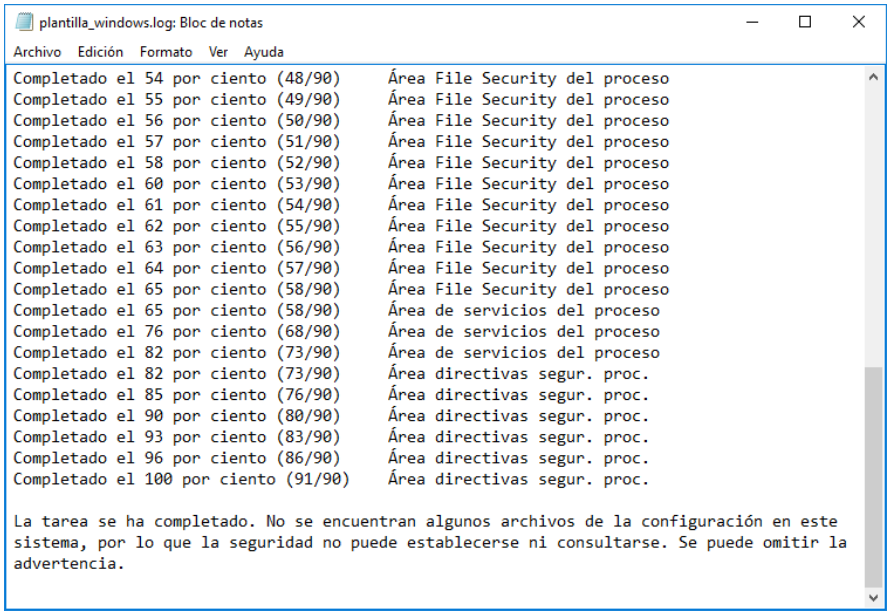
Los pasos que se describen a continuación se realizarán en todos aquellos servidores Windows Server 2016, independientes a un dominio, que implementen servicios o información de categoría alta y que se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

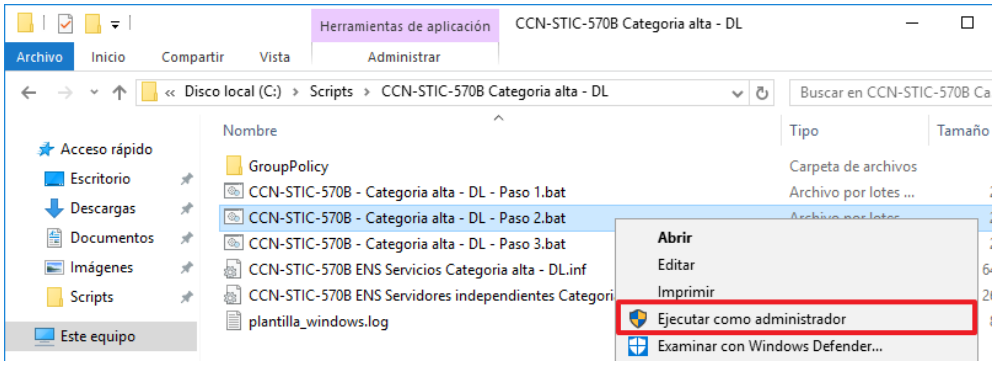
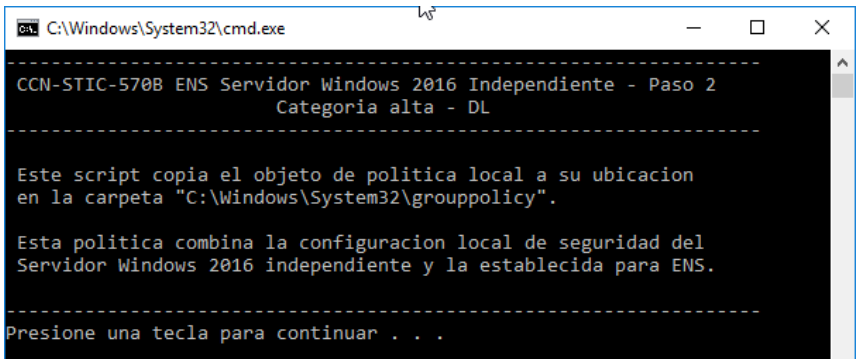
Paso	Descripción
1.	Inicie sesión en el servidor independiente donde se va aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del servidor.
3.	Cree el directorio “Scripts” en la unidad “C:\”.
4.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.

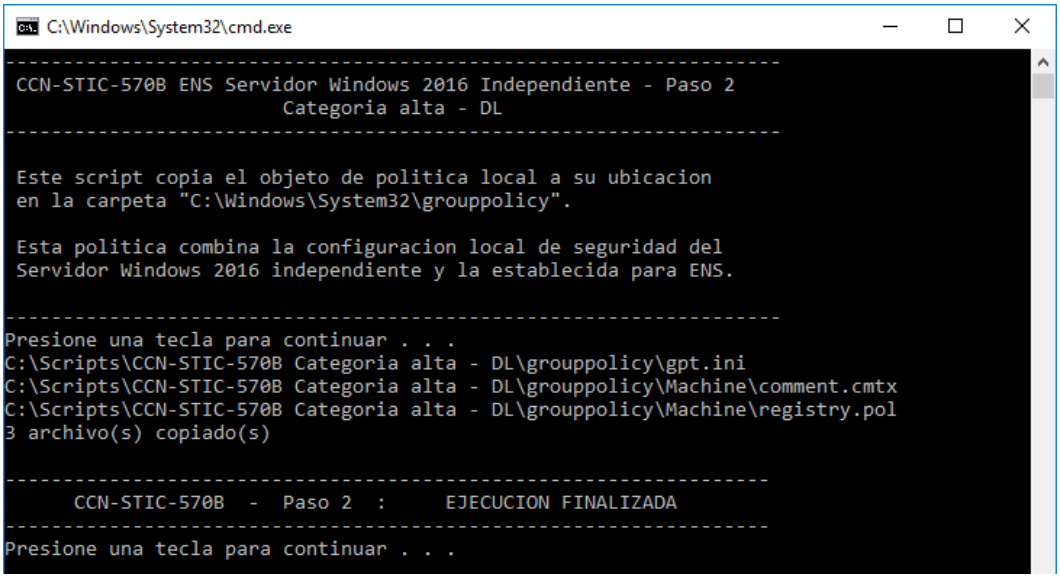
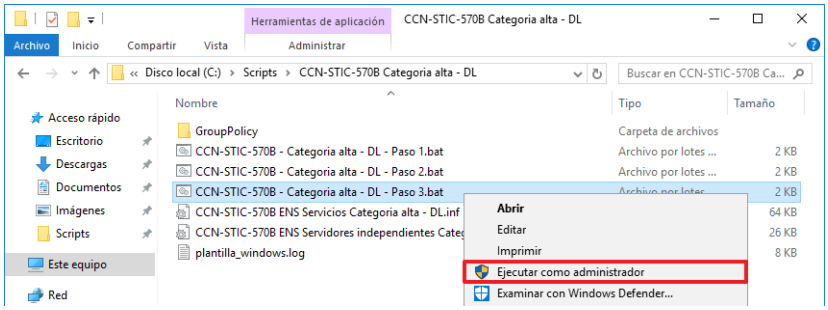
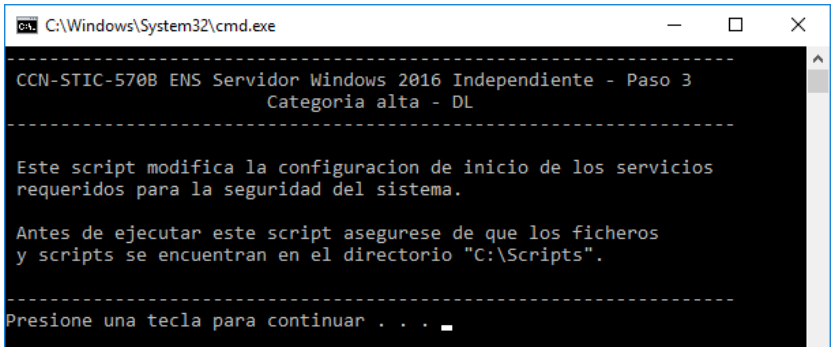
Paso	Descripción
5.	Abra la carpeta “CCN-STIC-570B Categoria alta - DL” que encontrará en la carpeta “C:\Scripts” que ha copiado. 
6.	Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos” oculta las extensiones conocidas 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”. 
7.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”. 

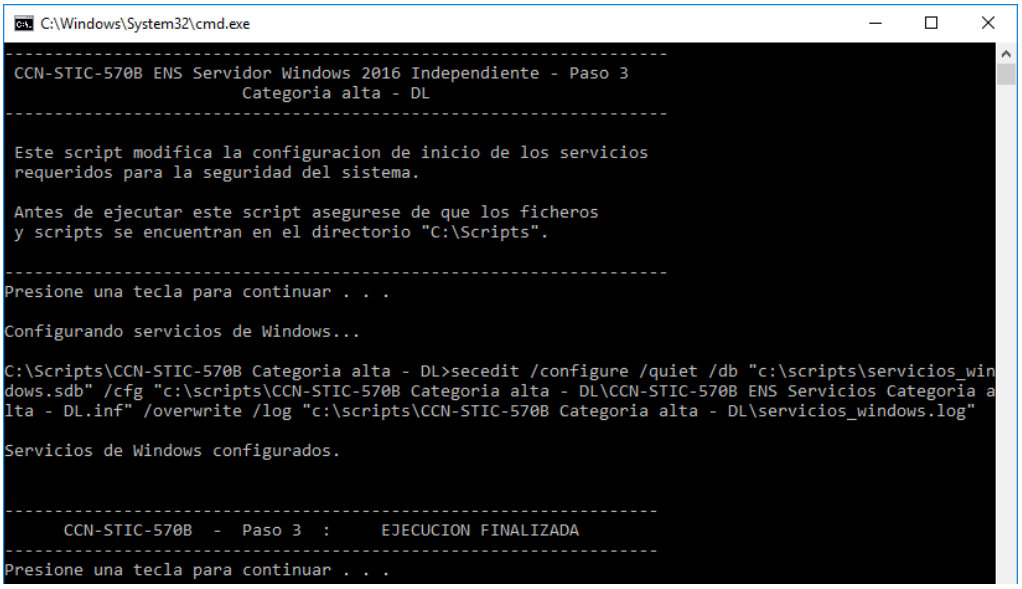
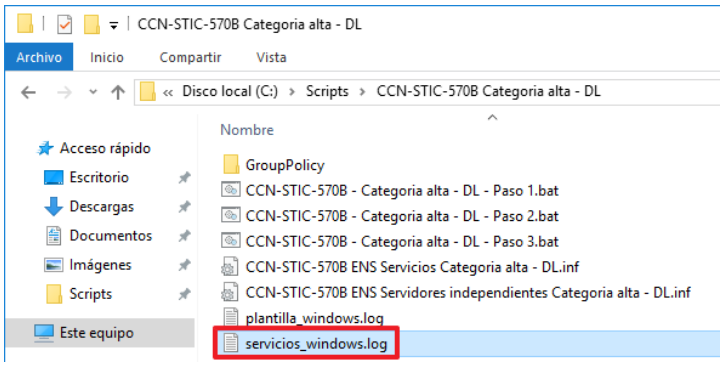
Paso	Descripción
8.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 
9.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio. – GroupPolicy (directorio) – CCN-STIC-570A Categoria alta – DL – Paso 1.bat – CCN-STIC-570A Categoria alta – DL – Paso 2.bat – CCN-STIC-570A Categoria alta – DL – Paso 3.bat – CCN-STIC-570A ENS Servicios Categoria alta - DL.inf – CCN-STIC-570A ENS Servidores independientes Categoria alta - DL.inf

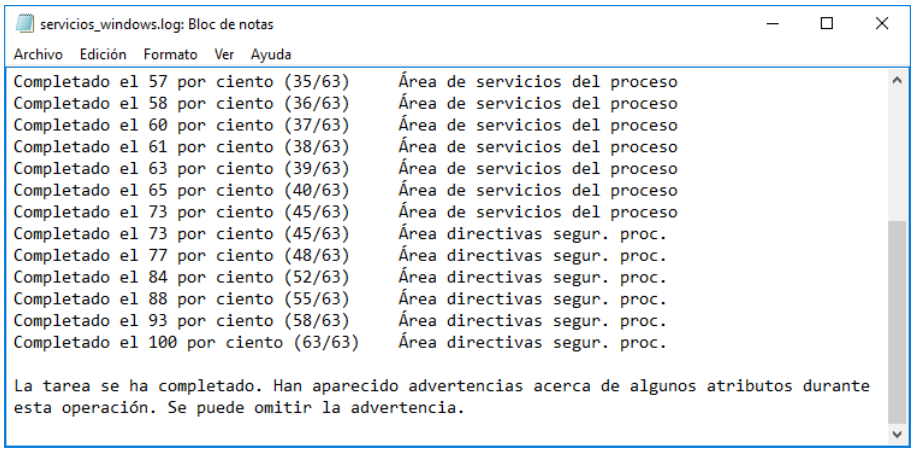
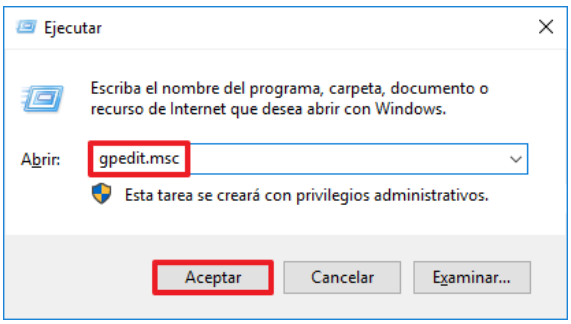
Paso	Descripción
10.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-570B – Categoria alta – DL – Paso 1.bat” y seleccione la opción “Ejecutar como administrador”.  **Nota:** En función del usuario administrador con el que haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que le solicite elevación de privilegios, introducir credenciales de la cuenta del usuario con los privilegios de administrador o bien eleve automáticamente los privilegios sin solicitarle nada.
11.	Pulse una tecla para iniciar la ejecución del script que configurará la plantilla de seguridad con la seguridad requerida para la categoría alta del ENS. 
12.	Una vez completado el proceso, deberá pulsar una tecla para continuar. 

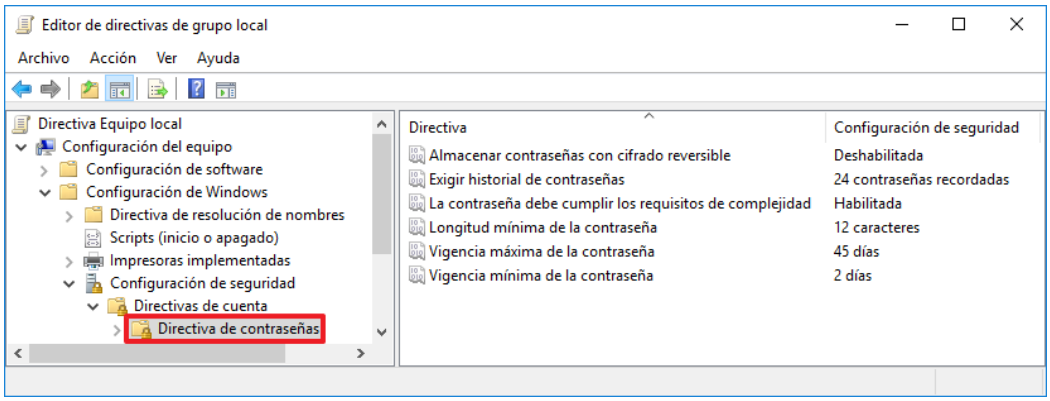
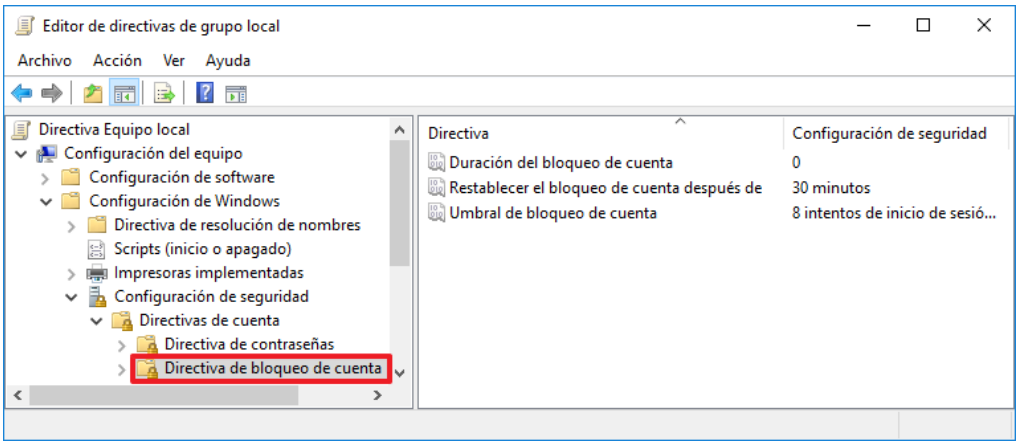
Paso	Descripción
13.	Pulse de nuevo otra tecla, para finalizar la ejecución del script. La ejecución del script genera un registro en la carpeta “C:\Scripts\CCN-STIC-570B Categoria alta - DL” con el nombre de “plantilla_windows.log”. 
14.	Abra este registro para comprobar si la configuración de la plantilla ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  **Nota:** En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script desde el paso 10.

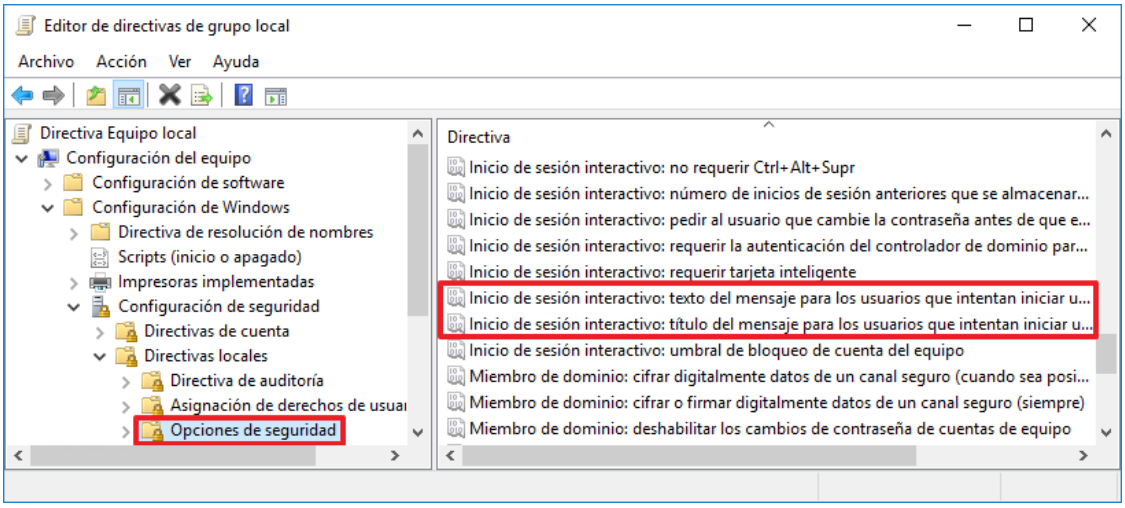
Paso	Descripción
15.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-570B – Categoria alta – DL – Paso 2.bat” y seleccione la opción “Ejecutar como administrador”.  **Nota:** En función del usuario administrador con el que haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que le solicite elevación de privilegios, introducir credenciales de la cuenta del usuario con los privilegios de administrador o bien eleve automáticamente los privilegios sin solicitarle nada.
16.	Pulse una tecla para iniciar la ejecución del script que configurará las plantillas administrativas con la seguridad requerida para la categoría alta del ENS. 

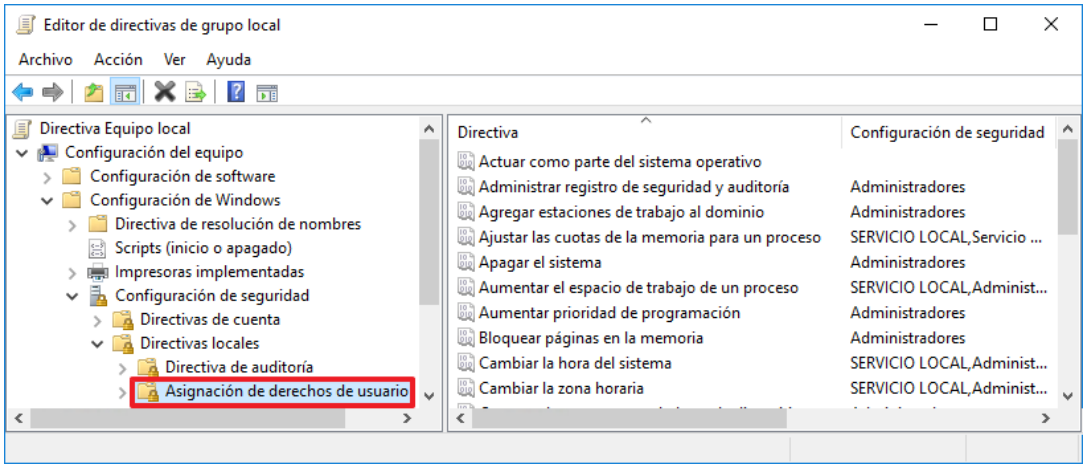
Paso	Descripción
17.	Una vez completado el proceso, deberá pulsar una tecla para continuar. 
18.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-570B – Categoria alta – DL – Paso 3.bat” y seleccione la opción “Ejecutar como administrador”.  **Nota:** En función del usuario administrador con el que haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que le solicite elevación de privilegios, introducir credenciales de la cuenta del usuario con los privilegios de administrador o bien eleve automáticamente los privilegios sin solicitarle nada.
19.	Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la categoría alta del ENS. 

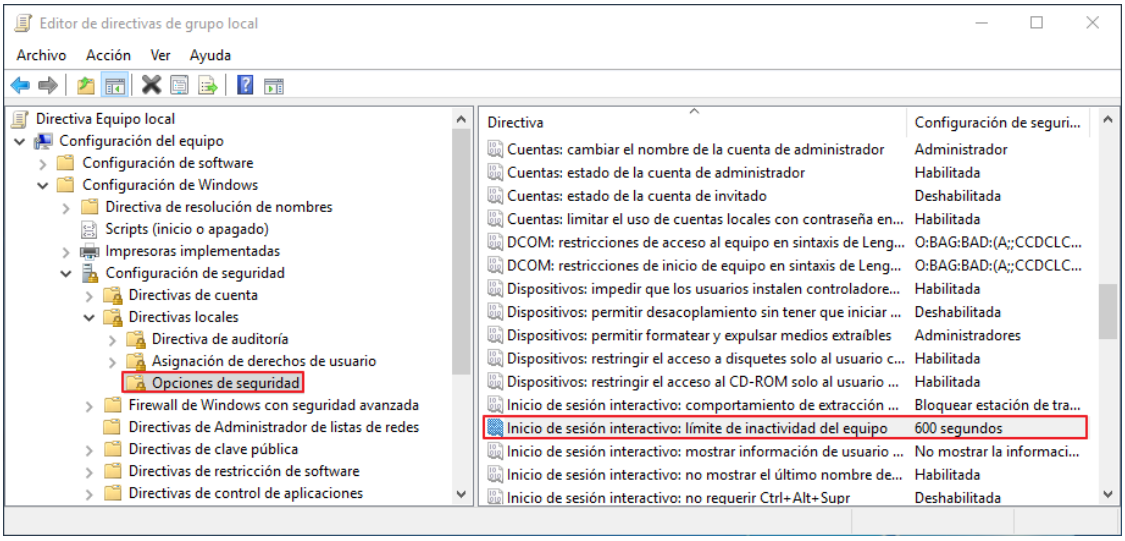
Paso	Descripción
20.	Una vez completado el proceso, deberá pulsar una tecla para continuar. 
21.	Pulse de nuevo otra tecla, para finalizar la ejecución del script. La ejecución del script genera un registro en la carpeta “C:\Scripts\CCN-STIC-570B Categoria alta – DL con el nombre de “servicios_windows.log”. 

Paso	Descripción
22.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  **Nota:** En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script desde el paso 18.
23.	Es factible que su organización cuente con una política de contraseña consolidada. La implementación de la política de categoría alta implementará una específica para los servidores con categoría alta. Deberá evaluarla para determinar si esta configuración le es válida o por el contrario debe adaptarla a las condiciones de su organización.
24.	Inicie el “Editor de directivas de grupo local”. Para ello, vaya al menú “Ejecutar” y escriba “gpedit.msc” y pulse “Aceptar”. **“Tecla Windows + R → gpedit.msc”** 

Paso	Descripción
25.	Despliegue la política y sitúese en la siguiente ruta. **"Directiva Equipo Local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseña"** 
26.	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.
27.	De forma similar a lo anterior, deberá evaluar la política de bloqueo de cuenta. Para ello y sin cerrar el editor, seleccione la "Directiva de bloqueo de cuenta" que encontrará al mismo nivel que la directiva de contraseñas. 
28.	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.

Paso	Descripción
29.	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.
30.	Para informar de las obligaciones sitúese en la siguiente ruta. **"Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"**
31.	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". 
32.	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.

Paso	Descripción
33.	Por último, la política de seguridad local especifica 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 haya asignado derechos determinados para la administración o gestión de los sistemas. Si esto fuera así deberá realizar las modificaciones sobre la configuración de política local.
34.	Despliegue la política y sitúese en la siguiente ruta. **"Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"** 
35.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
36.	Se establece a partir de la categoría media, según MP. EQ. 2 la necesidad de realizar el bloqueo del equipo ante un tiempo razonable de inactividad. A través de la política local aplicable sobre usuario, puede establecerse la medida de protección que habilita el salvapantallas y por lo tanto el bloqueo de la sesión. **Nota:** Si la organización presenta algún mecanismo 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
37.	Despliegue la política y sitúese en la siguiente ruta. **"Configuración de equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"** 
38.	Habilite y configure la siguiente directiva de seguridad: – Inicio de sesión interactivo: límite de actividad del equipo – Establezca el valor en 600 segundos (10 minutos).
39.	Cierre el "Editor de directivas de grupo local".
40.	Elimine la carpeta "C:\Scripts" y su contenido.
41.	Reinicie el servidor.

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

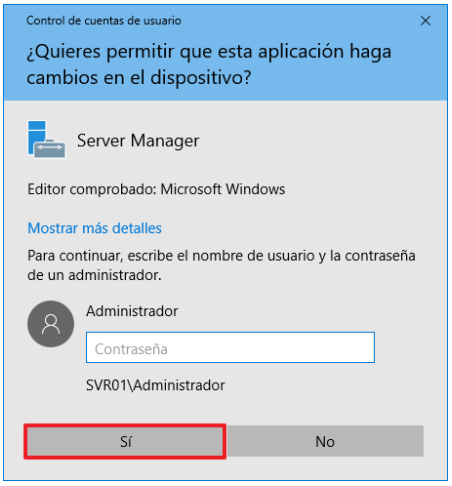
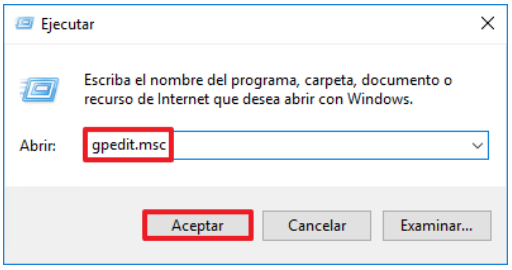
El control de cuentas de usuario surge, en Windows Vista, como respuesta para limitar las acciones de los administradores cuando actuaban con cuentas privilegiadas ante operativas que no requerían dicho privilegio. En sistemas previos a Windows Vista, un administrador que había iniciado una sesión actuaba 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.

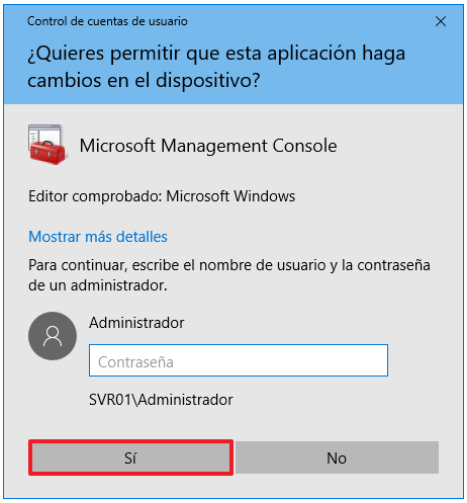
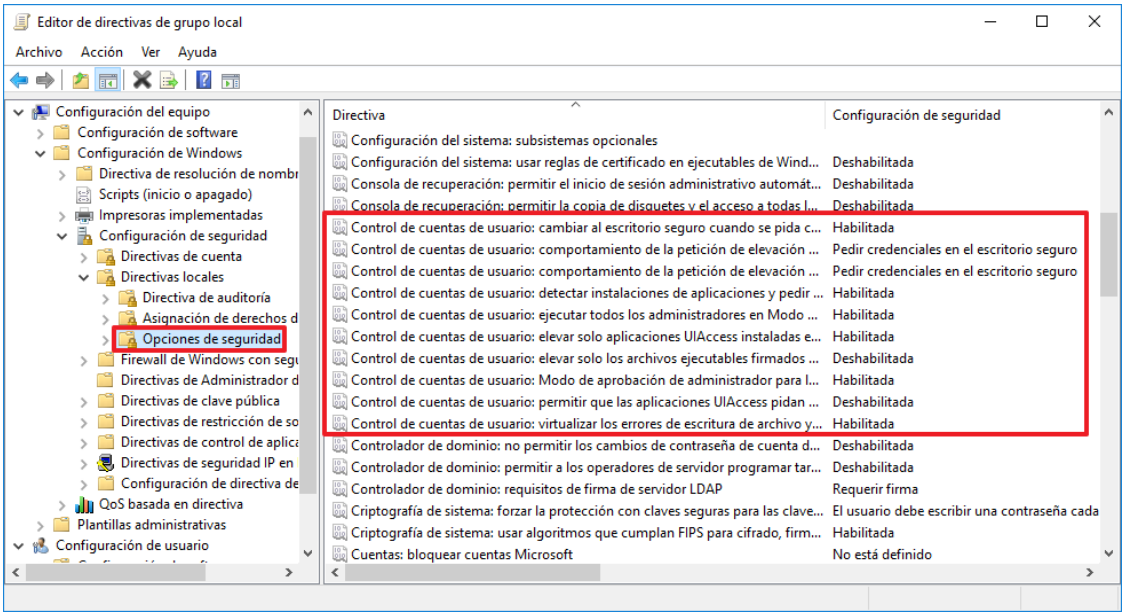
Siguiendo el principio de menor privilegio y menor exposición, la presente guía habilita las condiciones de funcionalidad de UAC para la categoría alta, aunque con los criterios más laxos de los aplicables.

No obstante, 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 modificación de la política local, de seguridad de aplicación a los servidores miembros, que pudieran presentar incidencias con la configuración de UAC.

Debe tenerse en cuenta 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.

Paso	Descripción
42.	Inicie sesión en el servidor independiente con una cuenta de administrador local. El sistema le solicitará elevación de privilegios para poder ejecutar la herramienta "Administrador del servidor". Pulse "Sí" para continuar. 
43.	Inicie el "Editor de directivas de grupo local". Para ello, vaya al menú "Ejecutar" y escriba "gpedit.msc" y pulse "Aceptar". **"Tecla Windows + R → gpedit.msc"** 

Paso	Descripción
44.	Pulse “Sí” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 
45.	Despliegue la política local y sitúese en la siguiente ruta. **“Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**
46.	Identifique las directivas relativas a “Control de cuenta de usuario”. 
47.	Realice las modificaciones oportunas.
48.	Cierre la política.

Paso	Descripción
49.	Reinicie el servidor. **Nota:** Debe tener en consideración que, si ha alterado la política de control de cuentas y ésta es menos rigurosa que la propuesta en la configuración deseada de 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.4.2. LISTA DE COMPROBACIÓN DE WINDOWS SERVER 2016 COMO SERVIDOR INDEPENDIENTE PARA LA CATEGORÍA ALTA

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 PASO A PASO DE IMPLEMENTACIÓN SEGURA DE WINDOWS SERVER 2016 COMO SERVIDOR INDEPENDIENTE PARA LA A".

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

Para realizar esta lista de comprobación deberá iniciar sesión en el servidor con una cuenta de usuario que tenga privilegios de administrador local.

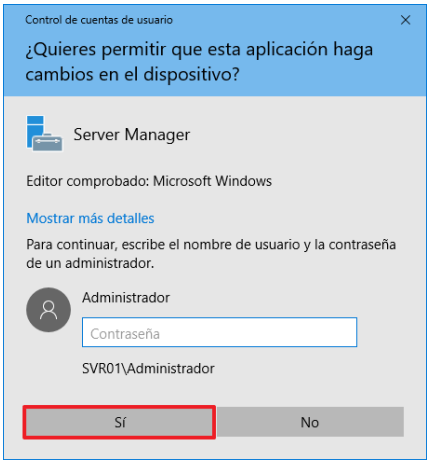
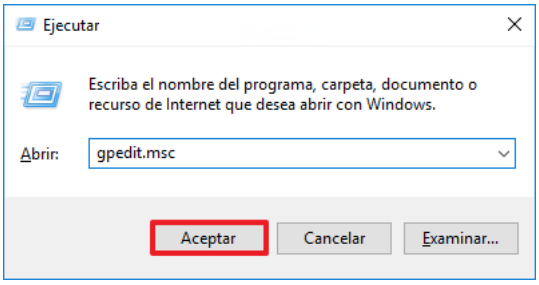
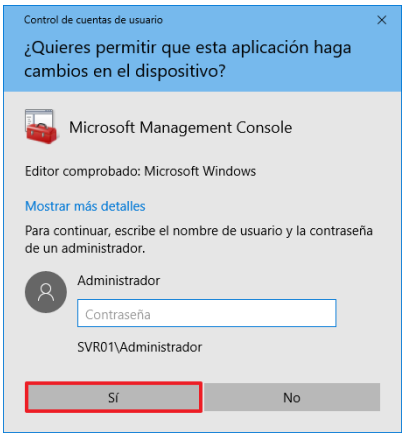
Para realizar las comprobaciones pertinentes en el servidor se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local. Las consolas y herramientas que se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

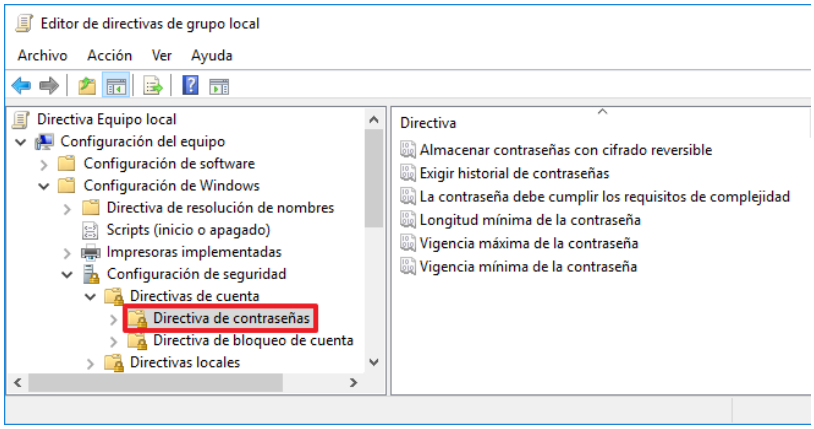
a) Editor de objetos de directiva de grupo local (gpedit.msc).

b) Editor de registro (regedit.exe).

c) Visor de Eventos (eventvwr.exe).

d) Servicios (services.msc).

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el servidor.		Inicie sesión en el servidor independiente con una cuenta de administrador local. El sistema le solicitará elevación de privilegios para poder ejecutar la herramienta "Administrador del servidor". Pulse "Sí" para continuar. 
2. Verifique la directiva de contraseñas en el editor de objetos de directiva de grupo local.		Inicie el "Editor de directivas de grupo local". Para ello, vaya al menú ejecutar y escriba "gpedit.msc" y pulse "Aceptar". **"Tecla Windows + R → gpedit.msc"**  Introduzca las credenciales de un usuario con privilegios de administrador y pulse "Sí" cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>En el “Editor de objetos de directiva de grupo local” seleccione el siguiente nodo:
“Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de contraseñas”
 
</td></tr>
<tr><td></td><td colspan="2"><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>12 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>
<tr><td>3. Verifique las directivas de bloqueo de cuenta en el editor de objetos de directiva de grupo local.</td><td></td><td>Seleccione el siguiente nodo:
“Directiva Equipo local → Configuración del Equipo → 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 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>4. Verifique las directivas de auditoría en el editor de objetos de directiva de grupo local.</td><td></td><td>Seleccione el siguiente nodo:
“Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”</td></tr>
<tr><td colspan="3">
<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>5. Verifique la asignación de derechos de usuario en el editor de objetos de directiva de grupo local.</td><td></td><td>Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → 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>
</table>
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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	
		Omitir comprobación de recorrido	Todos, SERVICIO LOCAL, Servicio de red, Administradores, Operadores de copia de seguridad, Usuarios, Windows Manager Group	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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	
6. Verifique las opciones de seguridad en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo: **"Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"**		

Directiva	Valor	OK/NOK
Acceso a redes: modelo de seguridad y uso compartido para cuentas locales	Clásico: usuarios locales se autentican con credenciales propias	
Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red	Habilitada	
Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Habilitada	
Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Habilitada	
Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	Deshabilitada	

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		System\CurrentControlSet\Control\ Print\Printers System\CurrentControlSet\Services\ EventLog Software\Microsoft\OLAP Server Software\Microsoft\WindowsNT\ CurrentVersion\Print Software\Microsoft\WindowsNT\ CurrentVersion\Windows System\CurrentControlSet\Control\ Content Index System\CurrentControlSet\Control\ Terminal Server System\CurrentControlSet\Control\ Terminal Server\UserConfig System\CurrentControlSet\Control\ Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\ Currente Version\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	
Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad		Habilitada	
Auditoría: auditar el acceso a objetos globales del sistema		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo

Directiva	Valor	OK/NOK
Auditoría: auditar el uso del privilegio de hacer 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	
Configuración del sistema: usar reglas de certificado en ejecutables de Windows para directivas de restricción de software	Deshabilitada	
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	
Control de cuentas de usuario: elevar sólo aplicaciones UIAccess instaladas en ubicaciones seguras	Habilitada	
Control de cuentas de usuario: elevar solo los archivos ejecutables firmados y validados	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		**Valor**	**OK/NOK**
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	
Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones Hash		Habilitada	
Cuentas: cambiar el nombre de cuenta de invitado		Invitado	
Cuentas: cambiar el nombre de la cuenta de administrador		Administrador	
Cuentas: estado de la cuenta de administrador		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;;CSW;;;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: 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 a 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 información del usuario	
Inicio de sesión: 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	
Inicio de sesión interactivo: requerir tarjeta inteligente		Deshabilitada	
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	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		**Valor**	**OK/NOK**
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	
Objetos del sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que no sean de Windows		Habilitada	
Seguridad de red: configurar tipos de cifrado permitidos para Kerberos		AES128_HMAC_SHA1, AES2656_HMAC_SHA1, Tipos de cifrados futuros	
Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión		Habilitada	
Seguridad de red: nivel de autenticación de LAN Manager		Enviar sólo respuesta NTLMv2 y rechazar LM y NTLM	
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		Requerir 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	

Comprobación	OK/NOK	Cómo hacerlo

Directiva	Valor	OK/NOK
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 de 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 de 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	

7. Verifique las directivas del almacén digital en el Editor de directivas de Grupo local.		Seleccione el siguiente nodo: **"Directiva Equipo Local → Configuración del Equipo → Plantillas administrativas → Componentes de Windows → Administración de derechos digitales de Windows Media"**

Directiva	Valor	OK/NOK
Impedir el acceso a Internet de Windows Media DRM	Habilitada	

8. Verifique las directivas del almacén digital en el Editor de directivas de Grupo local.		Seleccione el siguiente nodo: **"Directiva Equipo Local → Configuración del Equipo → Plantillas administrativas → Componentes de Windows → Almacén Digital"**

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

Comprobación	OK/NOK	Cómo hacerlo
9. Verifique las directivas del informe de errores de Windows en el Editor de directivas de Grupo local.		Seleccione el siguiente nodo: **"Directiva Equipo Local → Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Biometría"**

Directiva	Valor	OK/NOK
Permitir el uso de biometría	Habilitada	
Permitir que los usuarios de dominio inicien sesión mediante biometría	Habilitada	
Permitir que los usuarios inicien sesión mediante biometría	Habilitada	

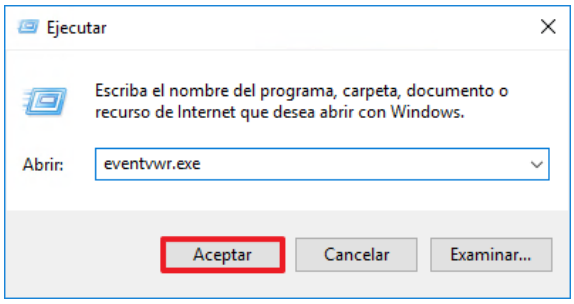
10. Verifique las directivas del informe de errores de Windows en el Editor de directivas de Grupo local.		Seleccione el siguiente nodo: **"Directiva Equipo Local → Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Directivas de reproducción automática"**

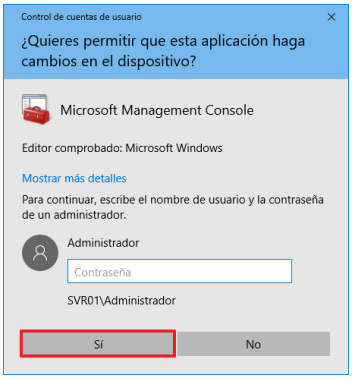
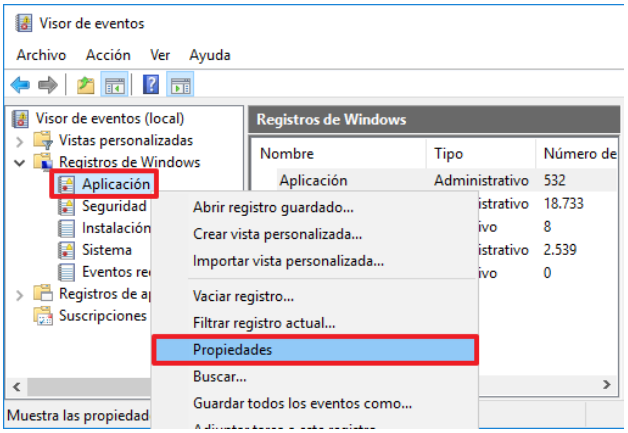
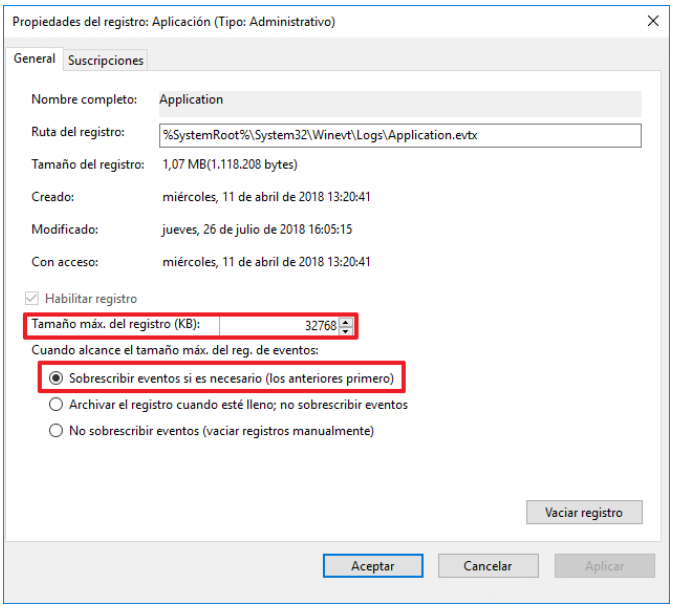
Directiva	Valor	OK/NOK
Establece el comportamiento predeterminado para la ejecución automática	Habilitado	
Desactivar reproducción automática	Habilitado	

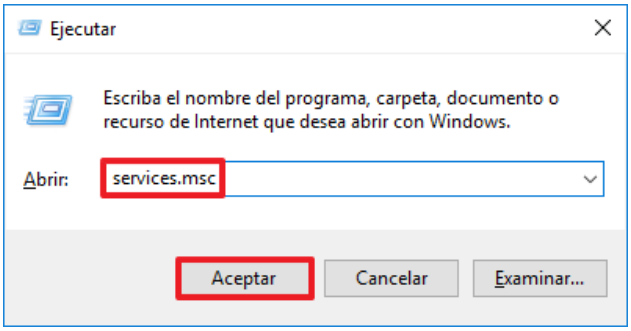
11. Verifique las directivas del informe de errores de Windows en el Editor de directivas de Grupo local.		Seleccione el siguiente nodo: **"Directiva Equipo Local → Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Informe de errores de Windows"**

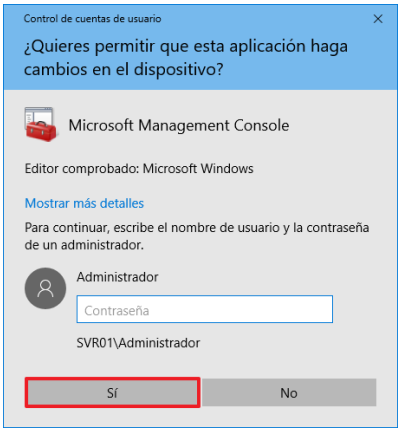
Directiva	Valor	OK/NOK
Deshabilitar el informe de errores de Windows	Habilitada	
No enviar datos adicionales	Habilitada	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td rowspan="4">12. Verifique las directivas del informe de errores de Windows en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → Plantillas Administrativas → 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">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>
<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 rowspan="3">13. Verifique las directivas del informe de errores de Windows en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Shell remoto de Windows”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Permitir acceso a Shell remoto</td><td>Deshabilitada</td><td></td></tr>
<tr><td rowspan="5">14. Verifique la configuración de la comunicación de Internet en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → Plantillas Administrativas → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Desactivar informe de errores de reconocimiento de escritura a mano</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar el Programa para la mejora de la experiencia de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar los vínculos “Events.asp” del Visor de eventos</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar el contenido “¿Sabía que…?” del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="7"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Desactivar la búsqueda en Microsoft Knowledge Base del Centro de ayuda y soporte técnico</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar el informe de errores de Windows</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar la actualización de archivos de contenido del Asistente para búsqueda</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar el acceso a la Tienda</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar la tarea de imágenes “Pedir copias fotográficas”</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="3">15. Verifique las directivas del informe de errores de Windows en el Editor de directivas de Grupo local.</td><td></td><td colspan="3">Seleccione el siguiente nodo:
“Directiva Equipo Local → Configuración del Equipo → Plantillas Administrativas → Sistema → Net Logon”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Permitir algoritmos de criptografía compatibles con Windows NT 4.0</td><td>Deshabilitada</td><td></td></tr>
<tr><td>16. Verifique la configuración del registro de eventos en el editor de objetos de directiva de grupo local.</td><td></td><td colspan="3">Inicie el “Visor de eventos”. Para ello, vaya al menú ejecutar, escriba “eventvwr.exe” y pulse “Aceptar”.
“Tecla Windows + R →eventvwr.exe”
 
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
		El “Control de cuentas de usuario” solicitará elevación de privilegios. Introduzca las credenciales de un usuario con privilegios de administrador y pulse “Sí” para continuar.  En el “Visor de eventos” despliegue el contenedor “Registros de Windows” y seleccione propiedades haciendo clic derecho sobre “Aplicación”.   Repita el proceso para “Seguridad” y “Sistema”.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="7"></td><td rowspan="7"></td><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Cuando alcance el tamaño máximo del registro de eventos de la aplicación</td><td>Sobrescribir eventos si es necesario (los anteriores primero)</td><td></td></tr>
<tr><td>Tamaño máximo del registro de la aplicación</td><td>32768 kilobytes</td><td></td></tr>
<tr><td>Cuando alcance el tamaño máximo del registro de eventos de seguridad</td><td>Sobrescribir eventos si es necesario (los anteriores primero)</td><td></td></tr>
<tr><td>Tamaño máximo del registro de seguridad</td><td>163840 kilobytes</td><td></td></tr>
<tr><td>Cuando alcance el tamaño máximo del registro de eventos del sistema</td><td>Sobrescribir eventos si es necesario (los anteriores primero)</td><td></td></tr>
<tr><td>Tamaño máximo del registro del sistema</td><td>32768 kilobytes</td><td></td></tr>
<tr><td>17. Verifique el modo de configuración de los servicios del sistema</td><td></td><td colspan="3">Inicie la consola de “Servicios”. Para ello, vaya al menú ejecutar, escriba “services.msc” y pulse “Aceptar”.
“Tecla Windows + R →services.msc”
 
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
		El "Control de cuentas de usuario" solicitará elevación de privilegios. Introduzca las credenciales de un usuario con privilegios de administrador y pulse "Sí" para continuar.  **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		
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado		
Adaptador de rendimiento de WMI	wmiApSrv	Manual		
Administración de aplicaciones	AppMgmt	Manual		
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado		
Administración de capas de almacenamiento	TieringEngineService	Manual		
Administración remota de Windows (WS-Management)	WinRM	Automático		
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual		
Administrador de conexiones de acceso remoto	RasMan	Manual		
Administrador de conexiones de Windows	Wcmsvc	Automático		

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

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

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

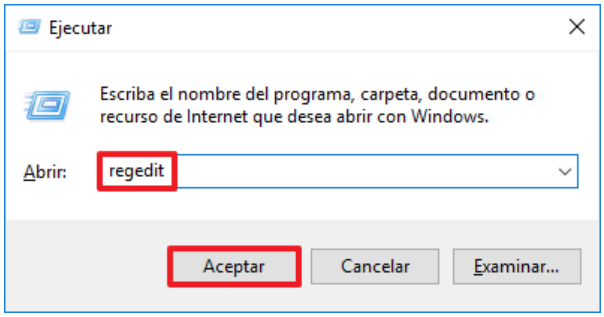
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Inicio de sesión secundario	seclogon	Deshabilitado		
Instalador de ActiveX (AxInstSV)	AxInstSV	Manual		
Instalador de módulos de Windows	TrustedInstaller	Manual		
Instantáneas de volumen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

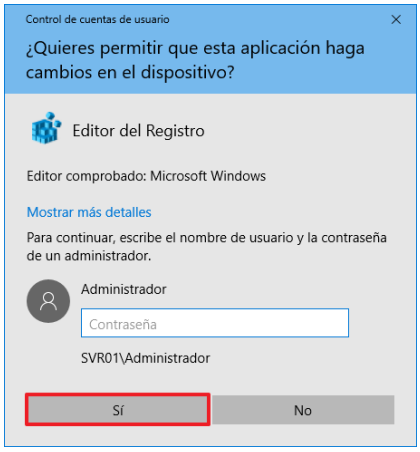
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Proveedor de instantáneas de software de Microsoft	swprv	Manual		
Publicación de recurso de detección de función	FDResPub	Deshabilitado		
Reconoc. ubicación de red	NlaSvc	Automático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

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

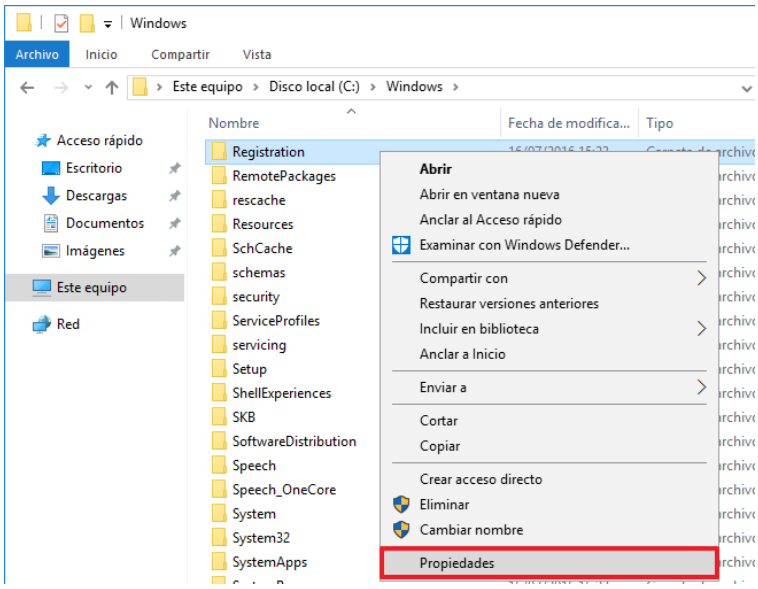
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de lista de redes	netprofm	Manual		
Servicio de notificación de eventos de sistema	SENS	Automático		
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService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

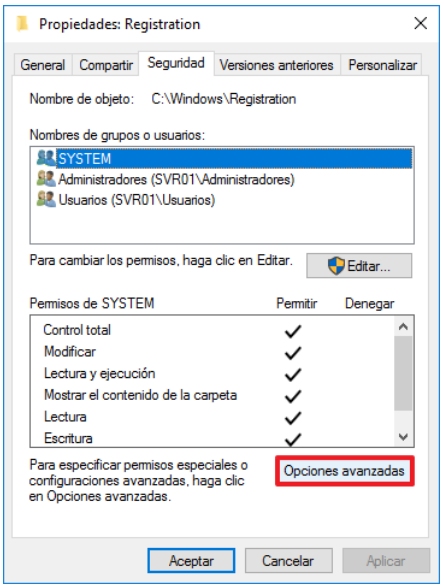
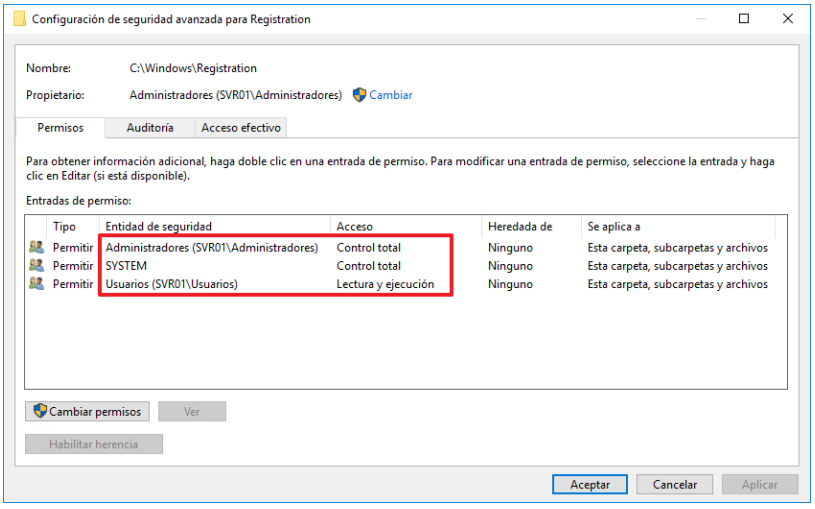
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual		
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado		
Servicio de Windows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

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servidor del modelo de datos del mosaico		tiledatamodelsvc	Automático		
Sincronizar host		OneSyncSvc	Automático		
Sistema de cifrado de archivos (EFS)		EFS	Manual		
Sistema de eventos COM+		EventSystem	Automático		
SMP de Espacios de almacenamiento de Microsoft		smphost	Manual		
Solicitante de instantáneas de volumen de Hyper-V		vmicvss	Manual		
Superfetch		SysMain	Manual		
Tarjeta inteligente		SCardSvr	Deshabilitado		
Telefonía		TapiSrv	Deshabilitado		
Telemetría y experiencias del usuario conectado		DiagTrack	Automático		
Temas		Themes	Deshabilitado		
Ubicador de llamada a procedimiento remoto (RPC)		RpcLocator	Manual		
WalletService		WalletService	Manual		
Windows Driver Foundation - User-mode Driver Framework		wudfsvc	Manual		
Windows Installer		msiserver	Manual		
Windows Search		WSearch	Deshabilitado		
Windows Update		wuauserv	Manual		
18. Verifique los valores del registro.		Compruebe los valores del registro mediante el uso del “Editor del Registro”. **“Windows+R → Regedit”** 			

Comprobación	OK/NOK	Cómo hacerlo
		El Control de cuentas de usuario solicitará elevación de privilegios. Introduzca las credenciales de un usuario con privilegios de administrador y pulse "Sí" para continuar. 

Directiva	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\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ ScreenSaverGracePeriod	0	
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\ KeepAliveTime	300000	
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\ PerformRouterDiscovery	0	

Comprobación	OK/NOK	Cómo hacerlo		
Directiva			**Valor**	**OK/NOK**
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	
19. Verifique los permisos asignados a ficheros y carpetas		Abra una ventana de Windows Explorer y diríjase a cada una de las rutas que indica el listado. Haga clic derecho con el ratón y seleccione “Propiedades” del menú.  **Nota:** Deberá tener cuidado para no realizar cambios sobre los permisos. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".		

Comprobación	OK/NOK	Cómo hacerlo
		En la pestaña “Seguridad”, seleccione “Opciones Avanzadas”.  En la pantalla resultante, compruebe los permisos asignados a cada carpeta o fichero.  **Nota:** Deberá tener cuidado para no realizar cambios sobre los permisos. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar". Al pulsar sobre opciones avanzadas, en la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios al pulsar sobre el botón “Continuar”. Pulse “Sí” para ver los permisos. 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		Administradores	Control total	
		System	Control total	
		Usuario	Leer y ejecución	
%SystemRoot%\system32\cacls.exe		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\clip.exe		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\rasadhlp.dll		Administradores	Control total	
%SystemRoot%\system32\rasauto.dll		Administradores	Control total	
%SystemRoot%\system32\rasautou.exe		Administradores	Control total	
%SystemRoot%\system32\raschap.dll		Administradores	Control total	
%SystemRoot%\system32\rasctrnm.h		Administradores	Control total	
%SystemRoot%\system32\rasctrs.dll		Administradores	Control total	
%SystemRoot%\system32\rasdial.exe		Administradores	Control total	
%SystemRoot%\system32\rasmans.dll		Administradores	Control total	
%SystemRoot%\system32\rasmontr.dll		Administradores	Control total	
%SystemRoot%\system32\rasphone.exe		Administradores	Control total	
%SystemRoot%\system32\rasppp.dll		Administradores	Control total	
%SystemRoot%\system32\rastapi.dll		Administradores	Control total	
%SystemRoot%\system32\runonce.exe		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\secedit.exe		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\tracert.exe		Administradores	Control total	
		System	Control total	

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 2012 R2 independientes. 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.

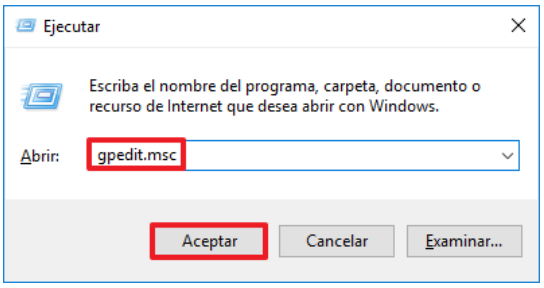
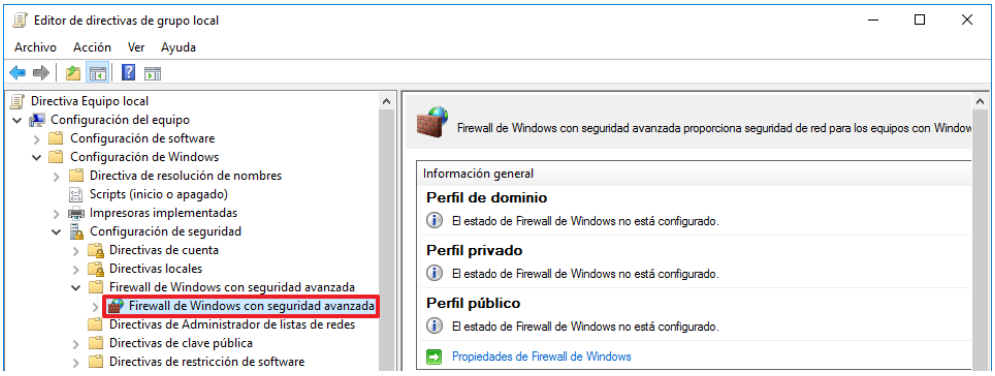
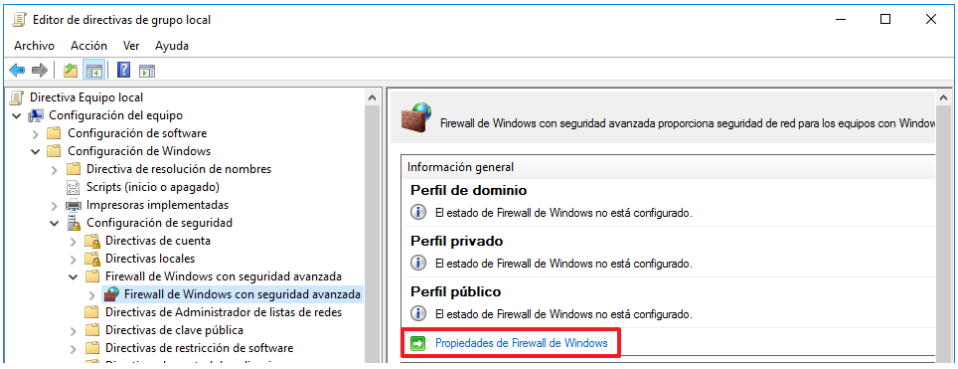
Debe tenerse en consideración que la implementación de un firewall de servidor independiente dependerá, en sí misma, de la funcionalidad del mismo y de los servicios que éste ofrece a la infraestructura. No tendrá, evidentemente, la misma funcionalidad y, por lo tanto, la necesidad de puertos abiertos, un servidor que actúe para dar soporte a sitios web que un servidor que mantenga bases de datos. A partir de Windows Vista, Microsoft proporciona un servicio de cortafuegos con seguridad avanzada. Éste permite realizar el control tanto de lo que entra como de lo que sale y para las diferentes categorías de redes en la que puede estar un sistema: pública, privada o dominio.

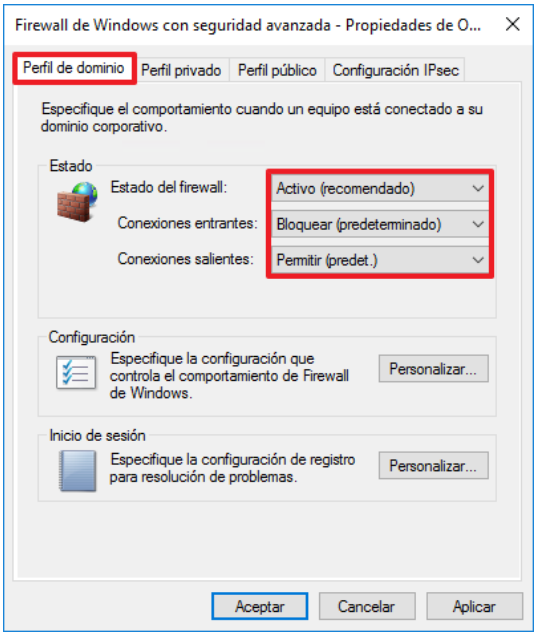
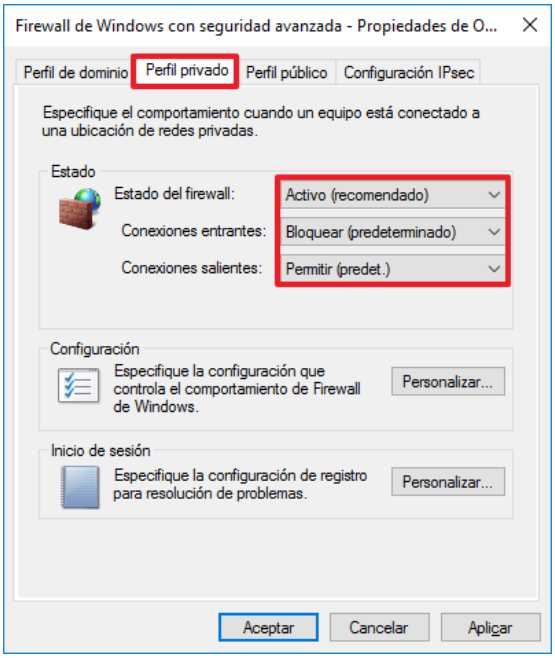
De forma predeterminada, el control de la configuración del cortafuegos con seguridad avanzada se establece a nivel local. No obstante, en un servidor independiente puede establecerse la configuración del mismo a través de la política local, de tal forma que, aunque se realizara una modificación del Firewall, a través de la consola local o bien mediante una modificación directa por código malicioso, a este le sería de aplicación la configuración establecida a través de la política local.

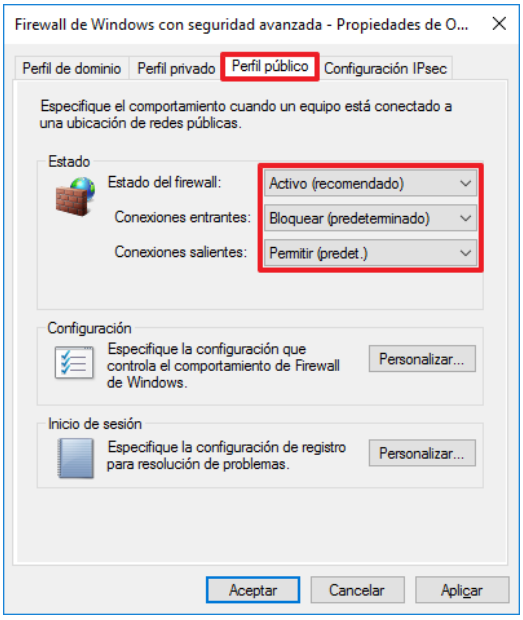
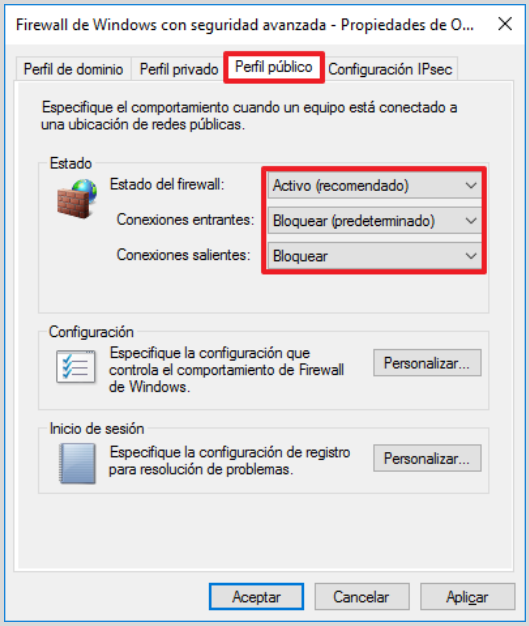
Teniendo en cuenta este hecho y a través de este anexo, se establecerá la configuración del cortafuegos mediante la aplicación de la política local. Como en los anexos previos, los operadores deberán realizar pruebas, en entornos de preproducción, antes de realizar una implementación en el entorno de producción.

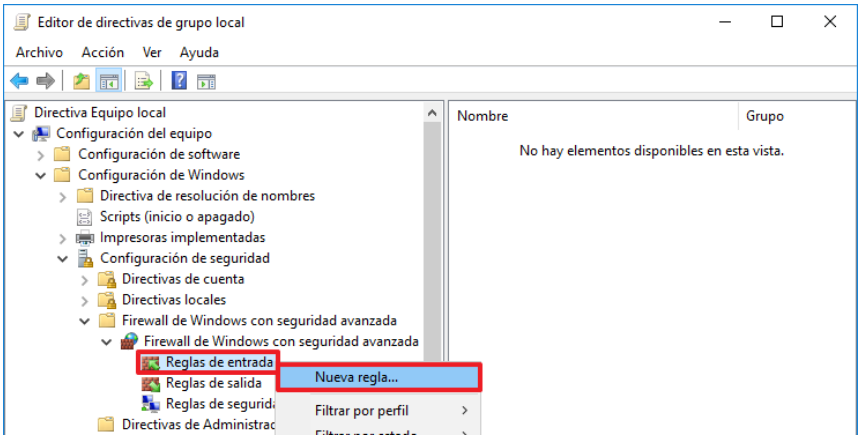
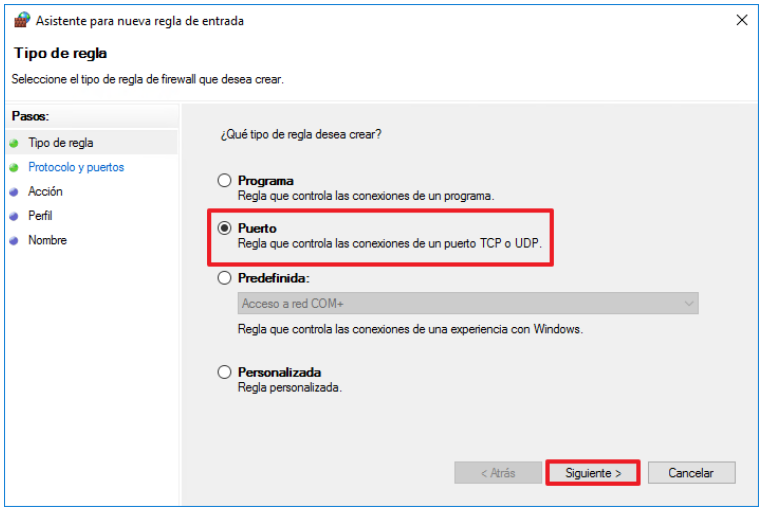
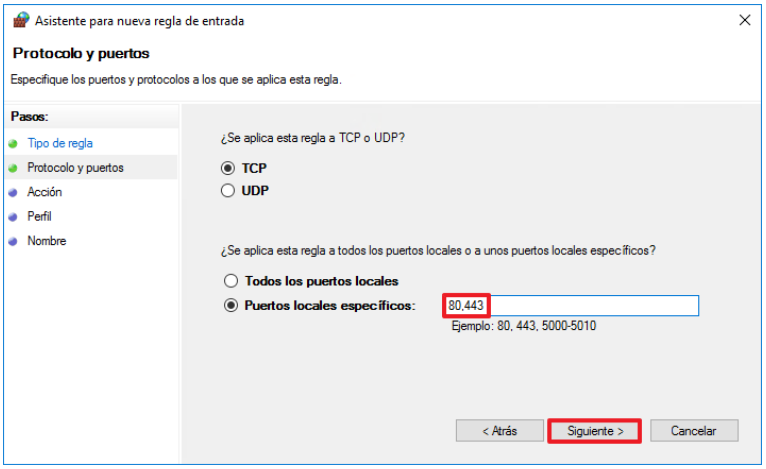
Nota: A modo de ejemplo, en este anexo se va a mostrar cómo configurar la política local, para la aplicación de seguridad de cortafuegos, para un conjunto de servidores web que sirven aplicaciones Web por puerto 80 y 443.

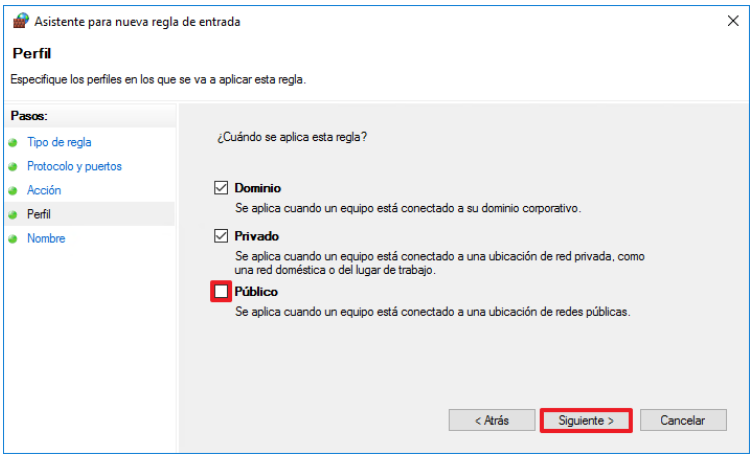
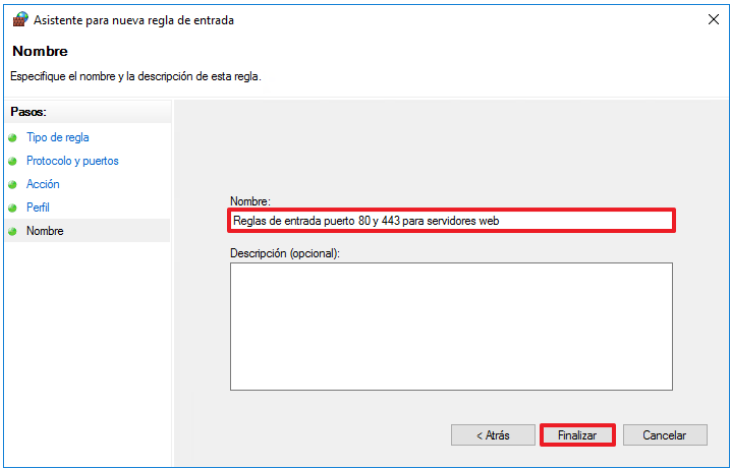
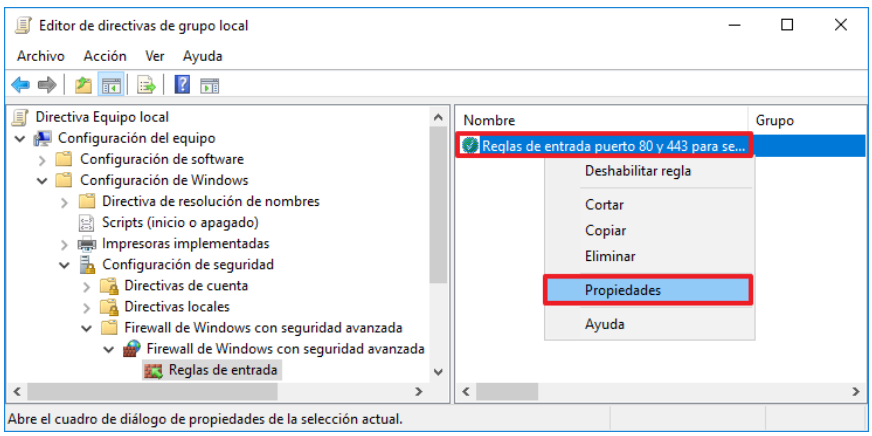
Paso	Descripción
1.	Inicie sesión con una cuenta de usuario que sea administrador local del servidor.

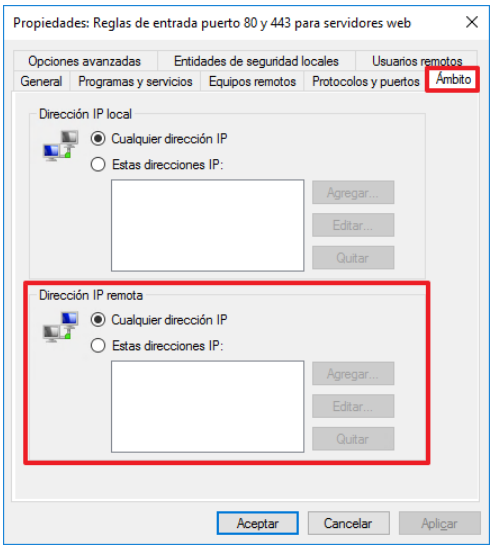
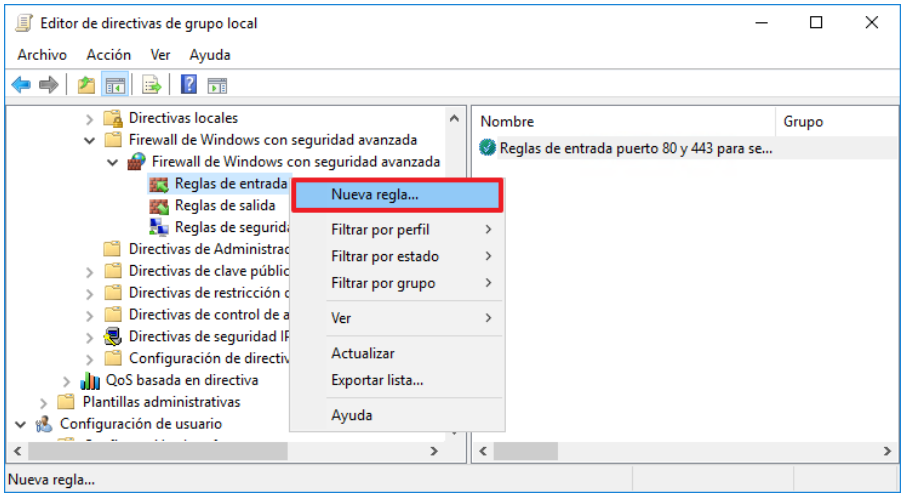
Paso	Descripción
2.	Inicie el “Editor de directivas de grupo local”. Para ello, vaya al menú ejecutar y escriba “gpedit.msc” y pulse “Aceptar”. **“Tecla Windows + R → gpedit.msc”**  **Nota:** En función de la categoría de seguridad que tenga implementado en el servidor se le solicitará bien la elevación de privilegios o bien la necesidad de introducir credenciales del usuario con privilegios de administrador.
3.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **“Directiva Equipo local → Configuración de equipo → Configuración de Windows → Configuración de seguridad → Firewall de Windows con seguridad avanzada → Firewall de Windows con seguridad avanzada”** 
4.	Pulse sobre las “Propiedades de Firewall de Windows” que aparecen en la configuración de “Información General”, existentes en el panel derecho. 

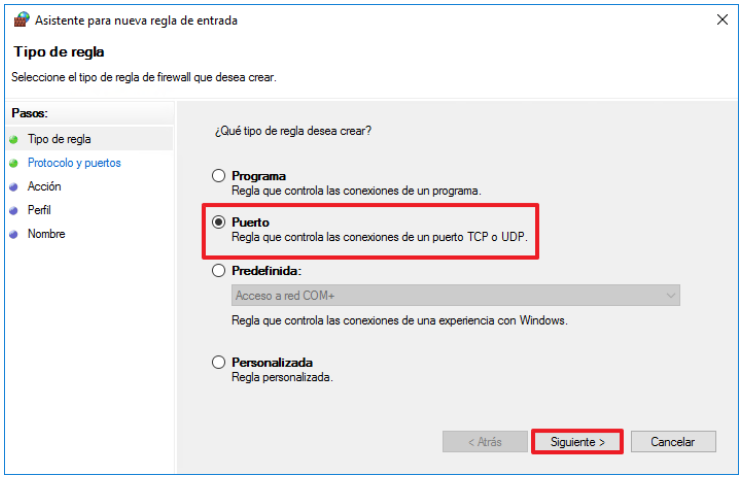
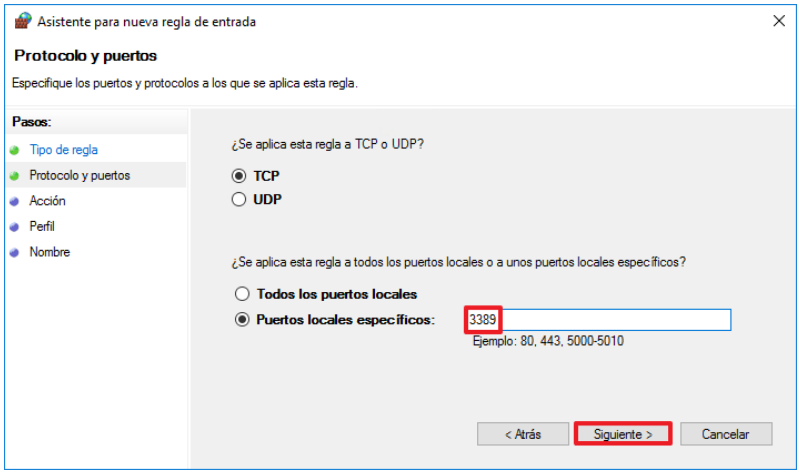
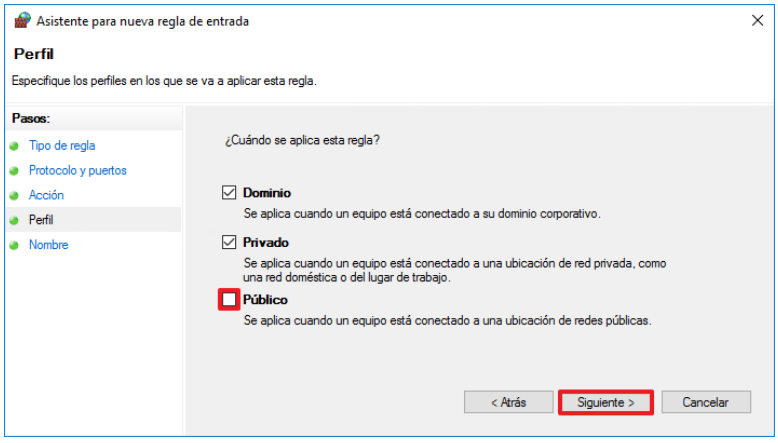
Paso	Descripción
5.	La primera de las pestañas “Perfil de dominio” configúrela como aparece en la siguiente imagen.  **Nota:** Debe tener en consideración que el presente servidor que está configurando es un servidor de tipo independiente y, por lo tanto, no formará parte de un dominio. No obstante podría ser adecuado establecer la configuración del dominio por si el servidor cambiara en algún momento su situación y este pasara a forma parte de un dominio.
6.	A continuación, vaya a la pestaña “Perfil privado”. Configúrela tal y como aparece en la siguiente imagen. 

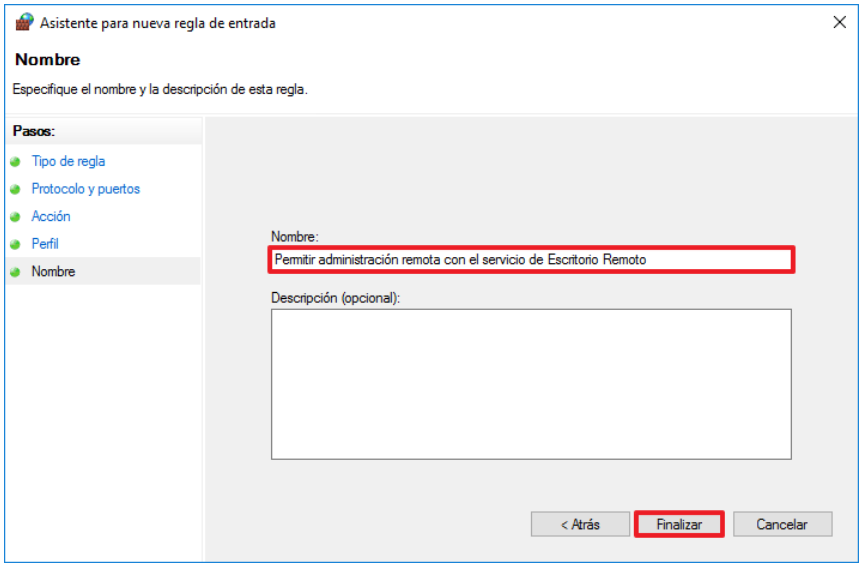
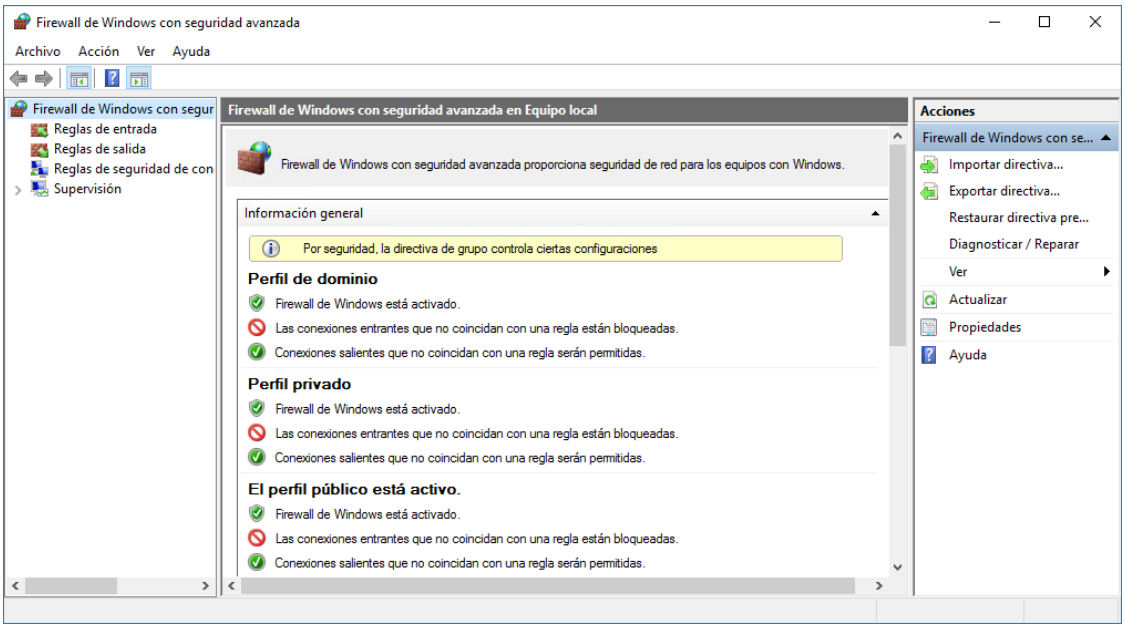
Paso	Descripción
7.	Vaya posteriormente a la pestaña “Perfil público” y establezca la configuración que aparece en la siguiente imagen.  **Nota:** En el caso de que los servidores proporcionaran servicios de categoría alta, sería recomendable que el perfil público quedara configurado como aparece en la siguiente imagen.  Verifique que la configuración de la conexión de red, con el que conecta el sistema a la red interna o a una DMZ, se encuentra en el perfil privado y no en perfil público.
8.	Pulse el botón “Aceptar” para guardar los cambios introducidos en los diferentes perfiles.
9.	Despliegue el “Firewall de Windows con seguridad avanzada” y vaya a “Reglas de entrada”.

Paso	Descripción
10.	Pulse con el botón derecho sobre “Reglas de entrada” y seleccione la opción “Nueva regla…”. 
11.	En el inicio del asistente seleccione la opción de “Puerto” y pulse el botón “Siguiente >”. 
12.	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 >”. 

Paso	Descripción
13.	En la pantalla de acción, mantenga la configuración y pulse el botón “Siguiente >”.
14.	En “Perfil”, deje marcados los perfiles “Dominio” y “Privado” y desmarque el perfil “público”. Pulse el botón “Siguiente >”. 
15.	Asigne un nombre a la nueva regla de entrada que está creando y pulse el botón “Finalizar”. 
16.	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
17.	Sería factible, por ejemplo, limitar 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. 
18.	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.
19.	Pulse nuevamente, con el botón derecho, sobre “Reglas de entrada” y seleccione nuevamente la opción “Nueva regla…”. 

Paso	Descripción
20.	En el inicio del asistente seleccione la opción de “Puerto” y pulse el botón “Siguiente >”. 
21.	En la opción de “Puertos locales específicos” introduzca “3389” y pulse el botón “Siguiente >”. 
22.	En la pantalla de acción, mantenga la configuración y pulse el botón “Siguiente >”.
23.	En “perfil”, deje marcados los perfiles “Dominio” y “Privado” y desmarque el perfil “público”. Pulse el botón “Siguiente >”. 

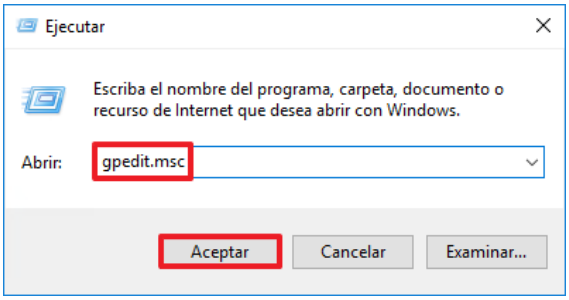
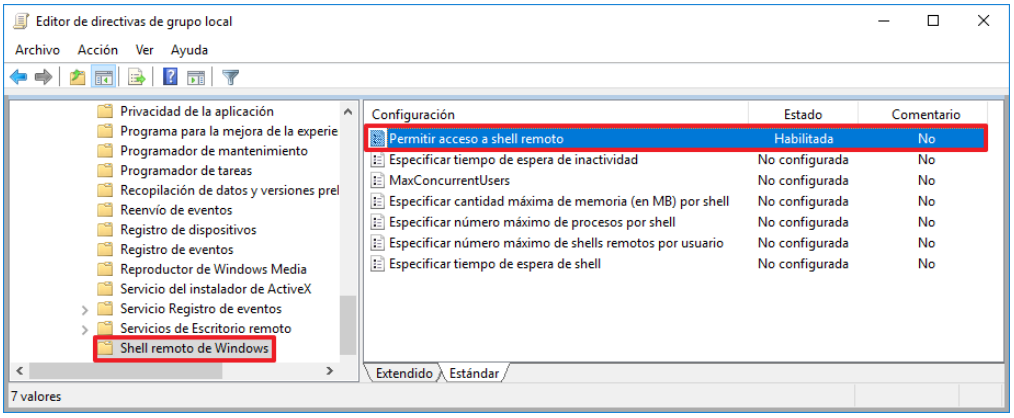
Paso	Descripción
24.	Asigne un nombre a la nueva regla de entrada que está creando y pulse el botón “Finalizar”. 
25.	Cierre la política de seguridad local. La configuración se habrá aplicado en el servidor y lo podrá comprobar ejecutando la configuración del servidor Firewall. Para ello podrá ejecutar desde el menú ejecutar la aplicación “WF.msc”. **“Tecla Windows + R → WF.msc”**  **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 de soporte de Microsoft referencia los puertos habitualmente usados por los servicios de Windows. *http://support.microsoft.com/default.aspx?scid=kb;EN-US;832017#method2*

ANEXO A.5.2. INSTALACIÓN DE ROLES ADICIONALES EN SERVIDOR INDEPENDIENTE QUE LE APLICAN A LA CATEGORÍA MEDIA Y ALTA DEL ENS

La categoría media y alta de la presente guía deshabilita 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 independiente, deberá editar la directiva correspondiente. Para ello, inicie la herramienta de "Administración de directivas de grupo local" mediante el menú "Ejecutar" y escriba "gpedit.msc" y pulse "Aceptar". **"Tecla Windows + R → gpedit.msc"** 
2.	Despliegue la política y sitúese en la siguiente ruta. **"Configuración de equipo → Plantillas Administrativas → Componentes de Windows → Shell remoto de Windows"**
3.	Seleccione la configuración de directiva denominada "Permitir acceso a Shell remoto de Windows" y configúrela para que queda "Habilitada". 

Paso	Descripción
4.	Cierre la política. **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 volver a deshabilitar la configuración de directiva denominada “Permitir acceso a Shell remoto de Windows”.