centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 578

IMPLEMENTACIÓN DEL ENS EN MICROSOFT HYPER-V SOBRE MICROSOFT WINDOWS SERVER 2016

FEBRERO 2019

MINISTERIO DE DEFENSA

Edita:

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2019.02.15 12:43:59 +01'00'

NIPO: 083-19-118-7
Fecha de Edición: febrero de 2019

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

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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.

febrero de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE HYPER-V EN EL ENS

ANEXO A.1. CONFIGURACIÓN SEGURA DE HYPER-V SOBRE UN SERVIDOR MIEMBRO DE DOMINIO CON SISTEMA OPERATIVO MICROSOFT WINDOWS SERVER 2016

1. APLICACIÓN DE MEDIDAS EN HYPER-V

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

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

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

a) Aplicación de seguridad en el entorno de Hyper-V sobre Microsoft Windows Server 2016 que pueda dar soporte a la organización y sobre el que se asientan muchos de los activos tecnológicos de dicha organización. Será, además, el mecanismo empleado para conducir la centralización y gestión de la seguridad.

b) Aplicación de seguridad en servidores miembro de dominio que sustentarán los diferentes servicios que prestara la organización, sujetos al RD 3/2010 y que se encontrarán implementados con Microsoft Windows Server 2016 implementados siguiendo la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016.

Nota: Así mismo, tenga en consideración que los sistemas operativos (y productos desplegados en ellos) correspondientes a las máquinas virtuales que albergue el servidor de Hyper-V deberán poseer un nivel de seguridad adecuado a su propósito teniendo en consideración la normativa aplicable. Es decir, si por ejemplo, dentro del servidor de Hyper-V se encuentra un máquina virtual que otorga el servicio de IIS, dicho sistema operativo deberá poseer la misma configuración de seguridad que si se tratase de un equipo físico al que se le aplica el ENS.

Para el análisis y desarrollo de las plantillas a aplicar, así como las tareas administrativas que sean necesarias para el cumplimiento de las medidas dispuestas en el ENS, se tienen en consideración los propios elementos técnicos que aporta Microsoft para el Servidor de Hyper-V, 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 éstas van a ser explicadas y además van a ser definidos los mecanismos que proporcione el sistema atendiendo a los criterios de categorización. Así se irá delimitando cada una

de las medidas y estableciendo en base a dicha categorización, que mecanismos se deberán habilitar para su cumplimiento. Habida cuenta de esta información dentro del directorio “Scripts” adjunto al presente documento se encuentran definidas 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 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 ya sean las propias máquinas virtuales o el propio servidor que administra dichas máquinas virtuales sin la debida autorización.

Adicionalmente se establece la necesidad de que el uso del sistema quede registrado para detectar y reaccionar ante una incidencia de seguridad o fallo del sistema.

Toda medida de control de acceso busca el equilibrio entre la usabilidad y la protección del sistema, de tal forma que la seguridad se irá incrementando en base a la categoría exigida. Por lo tanto, se requiere una menor exigencia de seguridad para la categoría básica mientras que en la categoría media y alta se requiere una mayor exigencia.

1.1.1.1. OP. ACC. 2. REQUISITOS DE ACCESO

Los requisitos de acceso se aplican desde la categoría básica y atenderán a la de necesidad proteger los recursos del sistema (ficheros, directorios y recursos compartidos) con algún mecanismo que impida su utilización, salvo a usuarios o perfiles de usuario que disfruten de los derechos de acceso suficientes.

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

Así mismo dicha persona responsable será la encargada de determinar aquellos recursos que serán compartidos y cuáles serán accesibles para los usuarios.

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 la 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 administración de un puesto de trabajo.

Es necesario en este sentido que el operador conozca los requerimientos y procesos para la asignación de las listas de control de acceso (ACL), teniendo en consideración que es la base en las infraestructuras Microsoft para la concesión o no de acceso, así como el que estará permitido o denegado en cada circunstancia La siguiente dirección URL facilita la información que proporciona el fabricante sobre los controles y vigilancia de acceso para Microsoft Windows Server 2016, incluyendo los controles de acceso dinámicos.

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

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

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

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

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.

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

Con respecto a los controles de auditoría o supervisión, se recomienda al operador de aquellas organizaciones que no contaran con sistemas de recolección, consolidación y tratamiento de eventos, la lectura y puesta en marcha de la guía "CCN-STIC-859 de recolección y consolidación de eventos" que aun habiendo sido emitida para Windows Server 2008 R2 es igualmente aplicable a sistemas Windows Server 2016. Aunque será mencionada a lo largo de la presente guía, con 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.

Así mismo es importante la creación de grupos con el objetivo de establecer los permisos a través de dichos grupos, permitiendo una gestión global y sencilla sobre el acceso a los recursos que ofrece Hyper-V. De este modo se evita modificar los permisos individuales de cada usuario para conceder o no permisos sobre un mismo recurso.

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

Altamente vinculado al punto "1.1.1.1 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 recurso 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, Microsoft Windows Server 2016 se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso que permitan determinar el derecho de acceso sobre los recursos que proporciona Hyper-V.

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

Se deberán establecer así mismo, niveles de control de acceso para impedir que un usuario no autorizado pueda visualizar contenido que no es requerido para las funciones que desempeña. Se establece por lo tanto a nivel de los recursos, el aplicar mecanismos de ACL para permitir la visualización de contenido o edición del mismo a los usuarios que los requieran exclusivamente.

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.

Se deberá tener en consideración debido a dicha norma que los permisos otorgados a los usuarios serán los mínimos requeridos no siendo necesario que estos posean permisos adicionales para la tarea que van a realizar. Por ejemplo, si un usuario tiene permiso para alterar el contenido de una carpeta no por ello implica que sea necesario que posea el permiso de "Control total". Con la concesión de este permiso se le estarían otorgando permisos más allá de las necesidades que requiere dicho usuario. Concederle el permiso de modificar se debe considerar como la opción más óptima desde el punto de vista del ENS.

1.1.1.4. 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 en un servidor Hyper-V antes de acceder a datos, es necesario indicar al sistema "quién eres" usando los métodos de autenticación existentes.

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. Los mecanismos de autenticación se deberán adecuar en función del nivel de criticidad de la información o el servicio web 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.

Debe tomarse en consideración que Hyper-V contempla los mecanismos de autenticación que otorga el propio Sistema Operativo sobre el que se soporta. A pesar de esto debe tomarse también en consideración que estos mecanismos son prolongados a las máquinas virtuales que sostiene el servicio de Hyper-V y que por lo tanto deben establecerse.

Del mismo modo deberá tener en consideración la diferencia de un servicio de Hyper-V que soporta un entorno de producción y un servicio de Hyper-V que soporta un entorno de preproducción debido a que la relevancia y repercusión no es la misma.

1.1.1.5. 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 que soportan el servicio de Hyper-V así como en las propias máquinas virtuales que contiene el servidor.

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 exigido.

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

1.1.1.6. 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.

El acceso al propio servidor de Hyper-V deberá ser realizado de forma segura, así como el realizado a las máquinas virtuales siempre que la organización considere necesario y apruebe dicho privilegio. El método de conexión habitual entre los sistemas Windows es “Escritorio Remoto” el cual deberá ser configurado acorde a lo descrito en el ENS:

a) En la categoría básica deberá garantizarse la seguridad del sistema cuando accedan remotamente usuarios u otras entidades, lo que implicará proteger tanto el acceso en sí mismo como la conexión.

b) En las categorías media y alta se establecerá una política específica que determine que es posible realizar de forma remota y que no, requiriendo una autenticación previa.

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. 1. INVENTARIO DE ACTIVOS

El ENS establece la necesidad a partir de su categoría básica la necesidad de mantener un inventario actualizado de todos los elementos del sistema identificando el responsable del mismo y detallando la funcionalidad del activo.

Debido a que el servidor de Hyper-V está destinado al almacenamiento de máquinas virtuales es necesario recopilar la información anteriormente requerida según el ENS. Por lo tanto, se requerirá conocer el número de máquinas virtuales que contiene el servidor, la función de cada una y el responsable asociado a dicha máquina.

1.1.2.2. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD

Se considera que el Servidor de Hyper-V debe configurarse previamente a su entrada en producción teniendo en cuenta las siguientes directrices:

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 no sean necesarias e incluso aquellas que sean inadecuadas para el fin que se persigue.

Para el cumplimiento de este principio, 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.

Estas mismas premisas deben extenderse a las máquinas virtuales contenidas por el propio servidor con el fin de mantener la misma seguridad que otorga el propio servidor de Hyper-V. Al igual que sucedía en apartados anteriores debe tenerse en consideración la diferencia de un servidor Hyper-V dedicado a la producción y un servidor Hyper-V para preproducción.

1.1.2.3. OP. EXP. 3. GESTIÓN DE LA CONFIGURACIÓN

Se deberá tener en consideración la configuración de los componentes del sistema que se gestione de forma que:

a) Se mantenga en todo momento la regla de funcionalidad mínima y seguridad por defecto.

b) El sistema debe adaptarse a las nuevas necesidades las cuales previamente han sido autorizadas y probadas en un entorno de pruebas antes de la puesta en producción.

c) El sistema debe reaccionar ante vulnerabilidades reportadas e incidentes.

Se establecerán mecanismos de uso de recursos con el fin de evitar una denegación de servicio debido al uso excesivo de elementos del servidor de Hyper-V. Del mismo modo se generarán configuraciones para las máquinas virtuales que permitan la estandarización de las mismas (conmutadores de red, discos, etc.).

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

Aplicable en las categorías media y alta de seguridad, se deberán implementar mecanismos para garantizar la trazabilidad de las acciones de los usuarios. Para ellos se deberá conocer:

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

b) Se incluirá la actividad de los usuarios y especialmente la de los operadores y administradores del sistema en cuanto pueden acceder a la configuración y actuar en el mantenimiento del mismo.

c) Deben registrarse las actividades realizadas con éxito, así como los intentos infructuosos.

d) La determinación de las actividades y con qué nivel de detalles, se determinará en base al análisis de riesgos que se haya realizado sobre el sistema.

e) La categoría alta requiere un sistema automatizado de recolección, consolidación y análisis de los registros de actividad.

El Servidor de Hyper-V, implementa mecanismos para la auditoría de acceso a objetos. El problema consiste en que de forma predeterminada los datos son almacenados localmente. Existen no obstante mecanismos nativos para la suscripción y recolección de evento. Ya comentado previamente, la guía CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2 permitirá establecer los procedimientos para la recogida y análisis de los registros de auditoria desde múltiples sistemas, permitiendo establecer así mecanismos de correlación.

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 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.

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

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

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

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

A través de controles centralizados en plantillas de seguridad, se establecerán mecanismos que controlen el acceso a los servidores Windows Server 2016 que contienen Hyper-V 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/threat-protection/windows-firewall/windows-firewall-with-advanced-security

1.2.1.2. MP. COM. 4. SEGREGACIÓN DE REDES

En la categoría alta del ENS se debe establecer una segregación de redes lo que acota el acceso a la información y, por consiguiente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren.

La red se segmentará en segmentos de forma que haya:

a) Control de entrada de los usuarios que llegan a cada segmento.

b) Control de salida de la información disponible en cada segmento.

c) Las redes se pueden segmentar por dispositivos físicos o lógicos. El punto de interconexión estará particularmente asegurado, mantenido y monitorizado.

Para atender a estas necesidades Hyper-V permite hacer uso de elementos denominados “Conmutadores de red” permitiendo la segregación y conexiones de las diferentes máquinas virtuales que el servidor posee.

1.2.2. PROTECCIÓN DE LA INFORMACIÓN

La protección de la información constituye el conjunto de medidas aplicadas sobre los servicios proporcionados, con el fin de proteger todo aquello que gestiona el servicio y que no es relativo a la configuración del servicio si no a los datos que este maneja o almacena.

1.2.2.1. MP. INFO. 3. CIFRADO

Tal y como define el ENS en la categoría alta es requerido el cifrado de la información durante su almacenamiento.

El servicio de Hyper-V dispone de mecanismos que permiten realizar un cifrado de los discos duros de cada máquina virtual cumpliendo así con el requisito establecido por el ENS.

1.2.2.2. MP. INFO. 9. COPIAS DE SEGURIDAD

Dentro del ENS ser establece a partir de su categoría básica la necesidad de realizar copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada.

Estas copias poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad, según proceda, de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

Las copias de seguridad deberán abarcar:

a) Información de trabajo de la organización.

b) Aplicaciones en explotación, incluyendo los sistemas operativos.

c) Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.

d) Claves utilizadas para preservar la confidencialidad de la información.

Para cumplir con dichas necesidades Hyper-V posee mecanismos que permiten guardar y recuperar máquinas virtuales con su correspondiente contenido.

2. RESUMEN Y APLICACIÓN DE MEDIDAS EN HYPER-V

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. 2	Requisitos de acceso	Revisión e implementación de mecanismos articulados en el Anexo A de la guía CCN-STIC-570A, adaptándolos a la organización.
OP. ACC. 3	Segregación de funciones y tareas	Revisión e implementación de guía CCN-STIC-578, adaptándolos a la organización.
OP. ACC. 4	Proceso de gestión de derechos de acceso	Revisión e implementación de guía CCN-STIC-578, adaptándolos a la organización.
OP. ACC. 5	Mecanismos de autenticación	Revisión e implementación de mecanismos articulados en el Anexo A de la guía CCN-STIC-570A, adaptándolos a la organización.
OP. ACC. 6	Acceso local	Revisión e implementación de mecanismos articulados en el Anexo A de la guía CCN-STIC-570A, adaptándolos a la organización. Revisión e implementación de guía CCN-STIC-578, adaptándolos a la organización.
OP. ACC. 7	Acceso remoto	Revisión e implementación de mecanismos articulados en el Anexo A de la guía CCN-STIC-570A, adaptándolos a la organización. Revisión e implementación de guía CCN-STIC-578, adaptándolos a la organización.
OP. EXP. 1	Inventario de activos	Revisión e implementación de guía CCN-STIC-578, adaptándolos a la organización.
OP. EXP. 2	Configuración de seguridad	Revisión e implementación de guía CCN-STIC-578, adaptándolos a la organización.
OP. EXP. 3	Gestión de la configuración	Revisión e implementación de guía CCN-STIC-578, adaptándolos a la organización.
OP. EXP. 8	Registro de actividad de los usuarios	Revisión e implementación de guía CCN-STIC-578, adaptándolos a la organización. Revisión e implementación de guía CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2
MP. COM. 3	Protección de la autenticidad y de la integridad	Revisión e implementación de guía CCN-STIC-578, adaptándolos a la organización.
MP. COM. 4	Segregación de redes	Revisión e implementación de guía CCN-STIC-578, adaptándolos a la organización.

Control	Medida	Mecanismo de aplicación
MP. INFO. 3	Cifrado	Revisión e implementación de guía CCN-STIC-578, adaptándolos a la organización.
MP. INFO. 9	Copias de seguridad	Revisión e implementación de guía CCN-STIC-578, adaptándolos a la organización.

ANEXO A.2. CATEGORÍA BÁSICA

ANEXO A.2.1. PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE HYPER-V SOBRE SERVIDORES WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen servidores de virtualización Hyper-V con una categorización de seguridad básica según los criterios del Esquema Nacional de Seguridad.

Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría básica, deberá realizar las implementaciones según se referencian en el presente anexo.

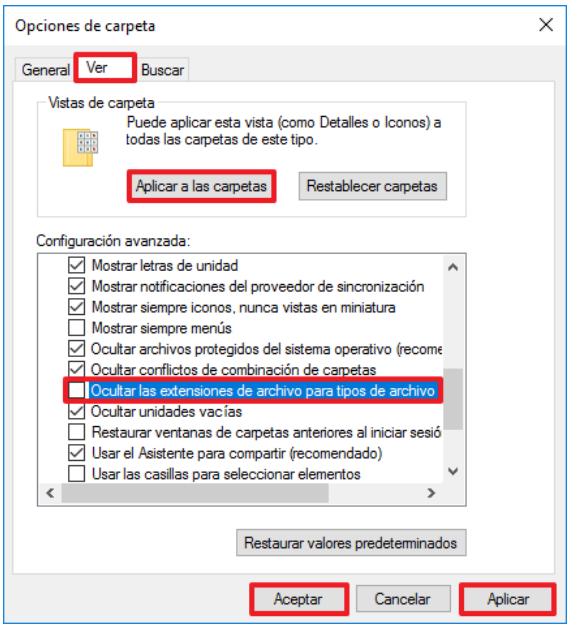
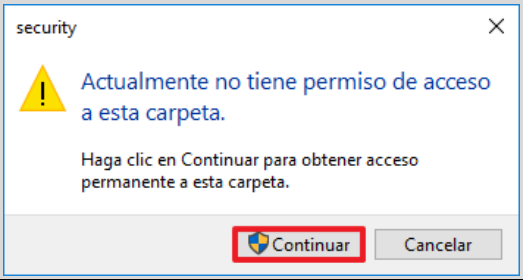
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

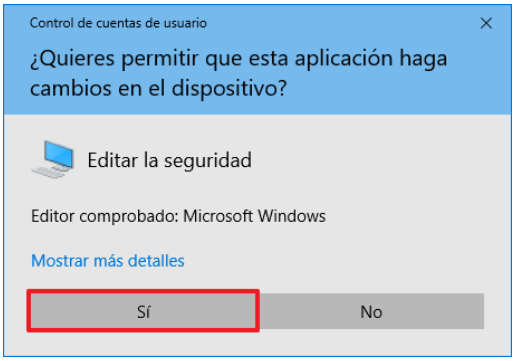
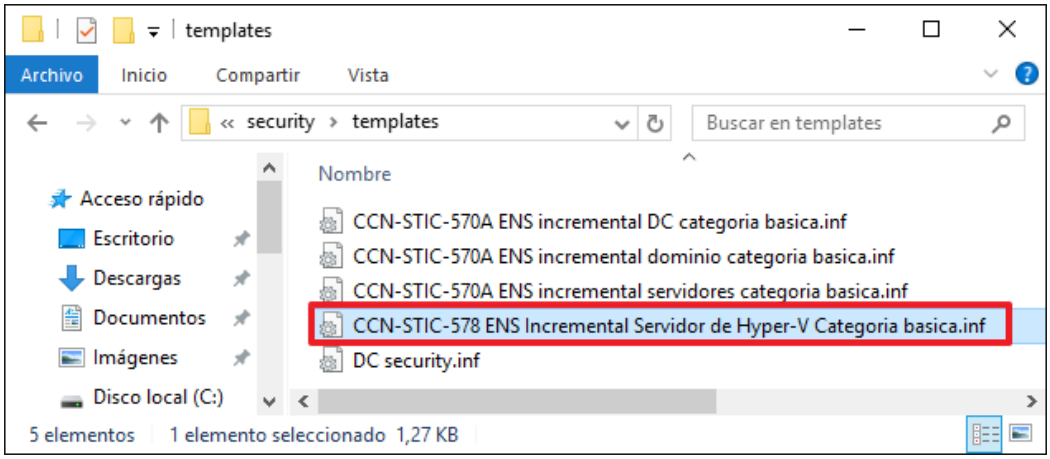
1. PREPARACIÓN DEL DOMINIO

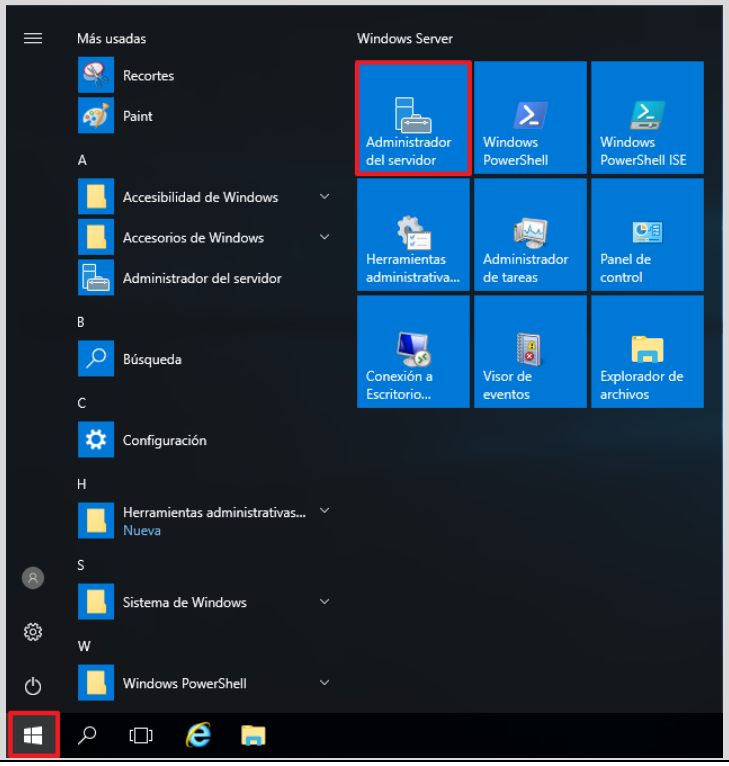
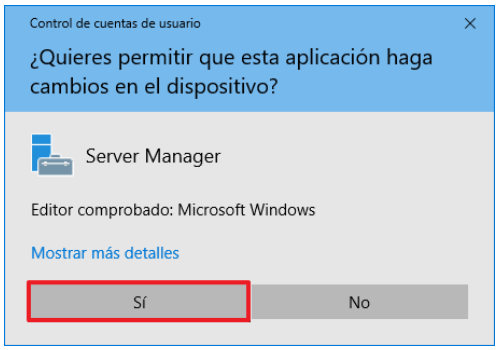
Los pasos que se describen a continuación deberá realizarlos en un Controlador de Dominio del dominio al que pertenece el equipo servidor que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer servidor de Hyper-V que actúe como miembro del dominio. Durante este procedimiento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

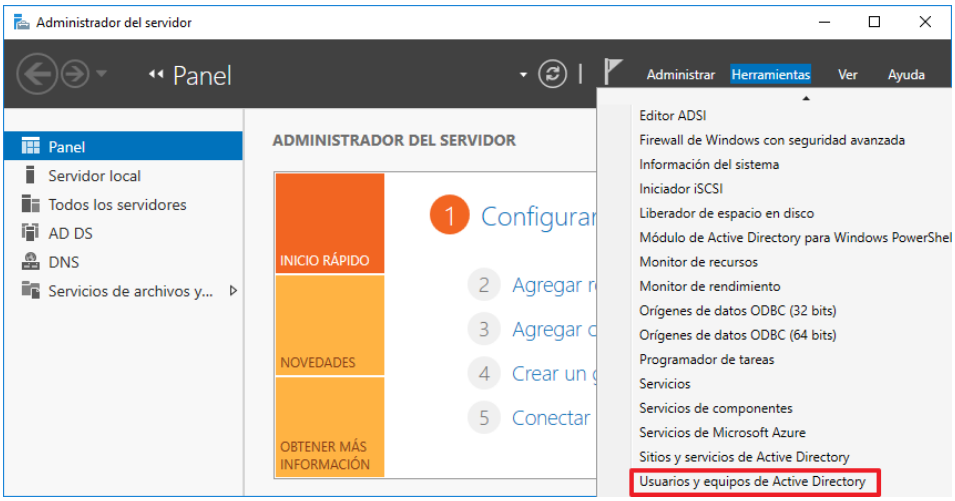
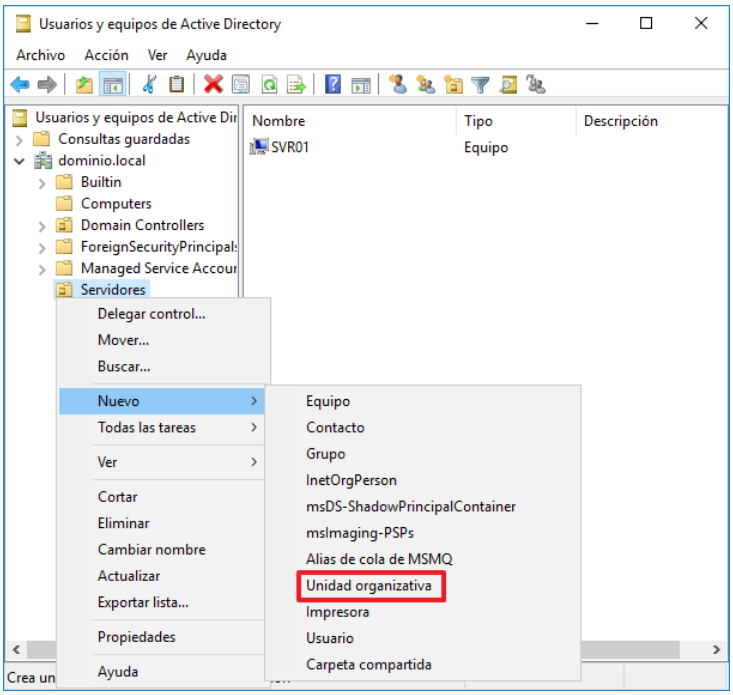
Nota: Esta guía asume que los servidores Controladores del Dominio al que pertenece el equipo servidor de Hyper-V que está asegurando, se les ha aplicado la configuración descrita en la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016". Si no es así, aplique la guía correspondiente al Controlador de Dominio, antes de continuar con la aplicación de ésta.

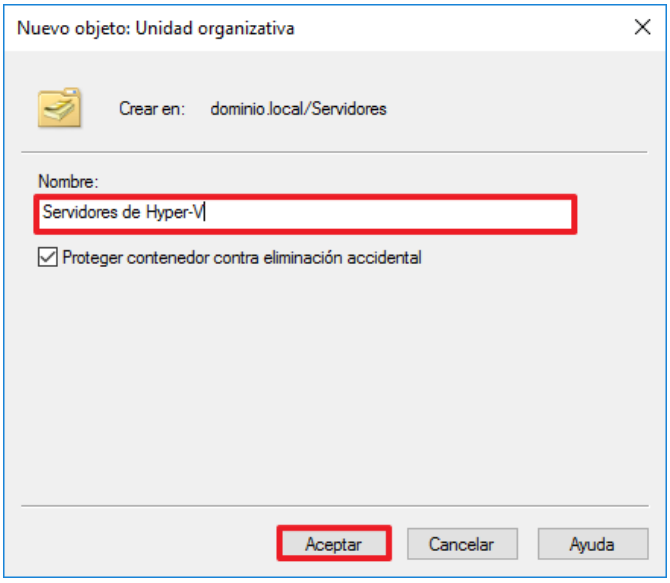
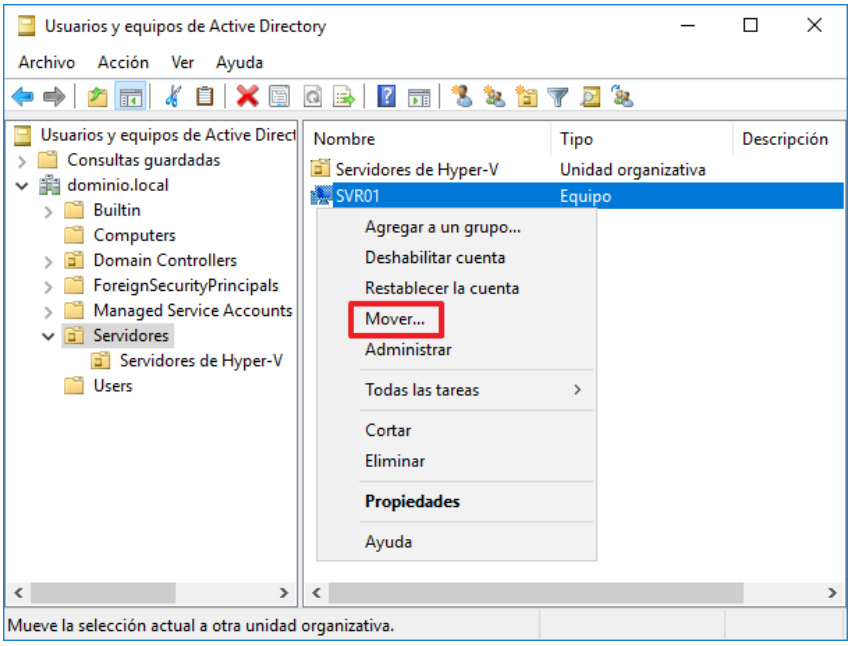
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
2.	Cree el directorio "Scripts" en la unidad "C:\". **Nota:** Los scripts asumen que su ubicación en el sistema será bajo "C:\Scripts". Si los colocara en otra ubicación, tendrá que editar los scripts para reflejar la nueva ubicación.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".

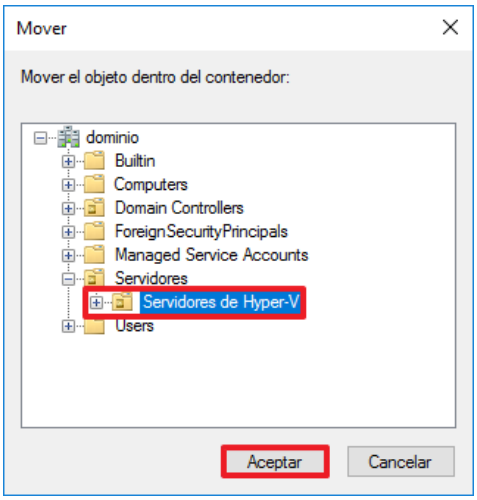
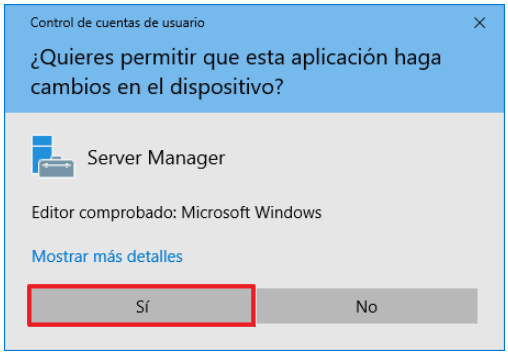
Paso	Descripción
4.	Si no lo ha hecho anteriormente, configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos.
5.	Para configurar el “Explorador de Windows” y que éste muestre las extensiones de todos los archivos, abra una ventana del “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. En la venta emergente, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la imagen.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación “¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?”, y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".
6.	Adicionalmente acceda al directorio “C:\Windows\Security\Templates”. **Nota:** Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón “Continuar” ante la ventana emergente. 

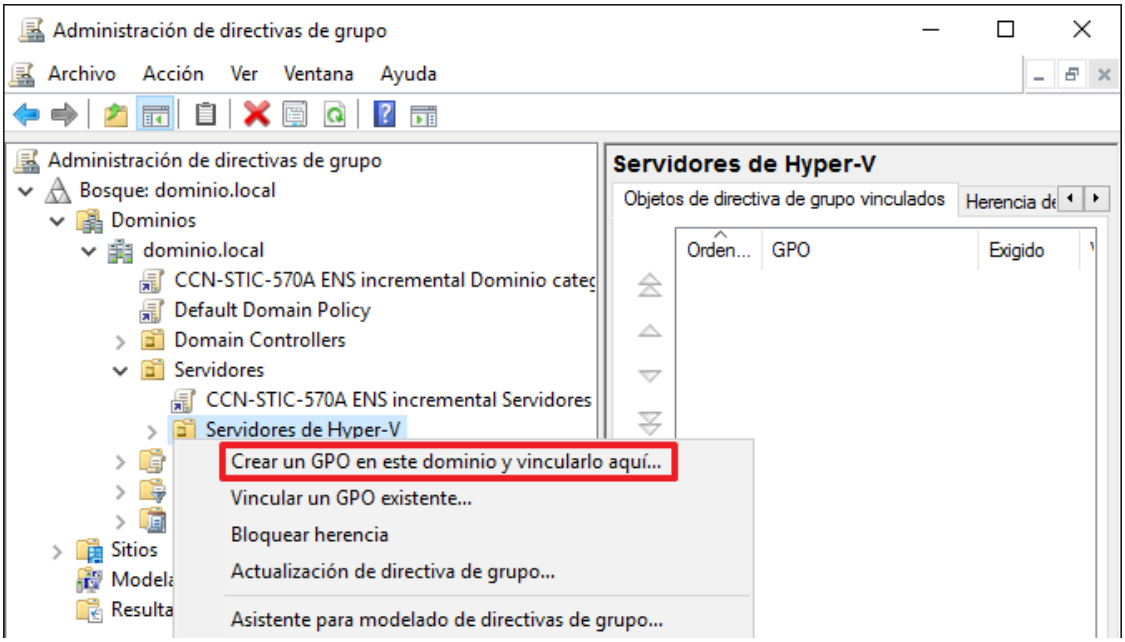
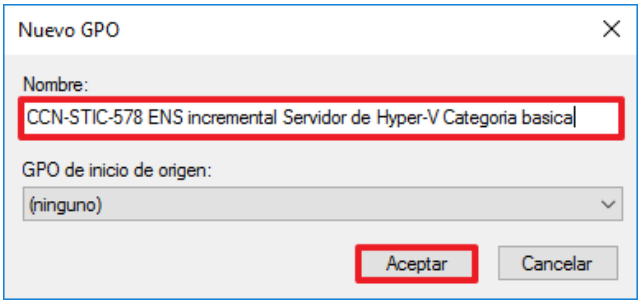
Paso	Descripción
7.	El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar. 
8.	Copie el fichero “CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria basica.inf” ubicado en “C:\Scripts” en el directorio “C:\Windows\Security\Templates”. 

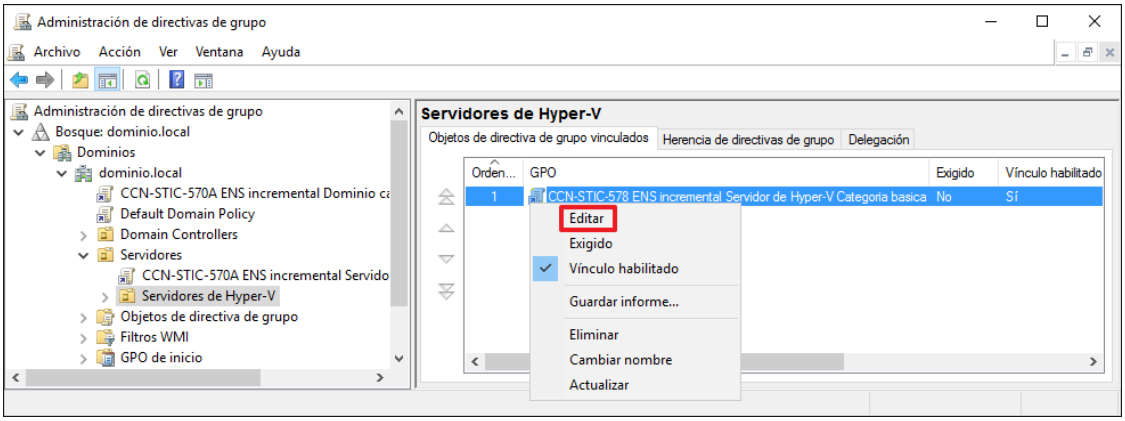
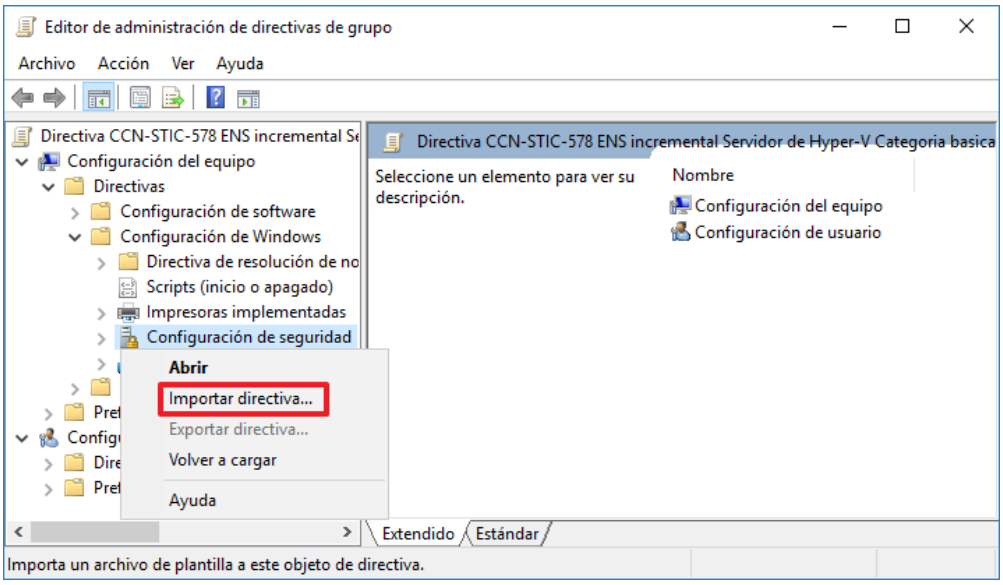
Paso	Descripción
9.	A continuación, deberá crear la unidad organizativa "Servidores de Hyper-V". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente.  **Nota:** Por defecto el "Administrador del servidor" se inicia cuando un usuario inicia sesión en el equipo. Si no se encuentra vinculado a la barrada de tareas podrá acceder a él en la ruta **"Inicio → Administrador del servidor"**. 
10.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 

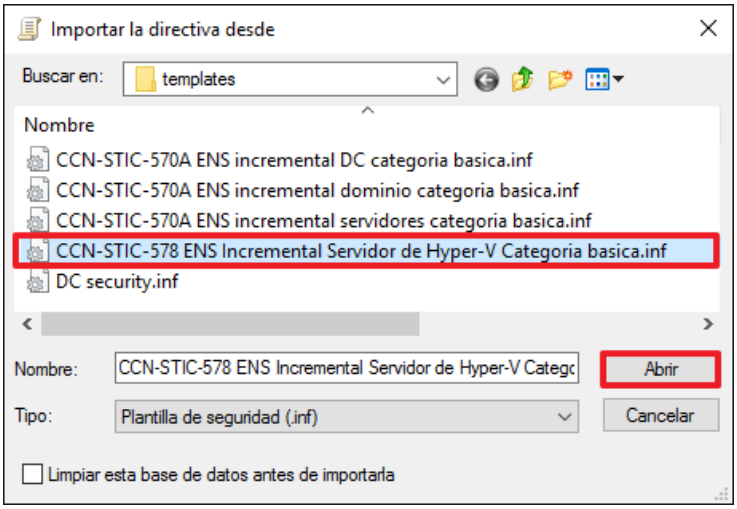
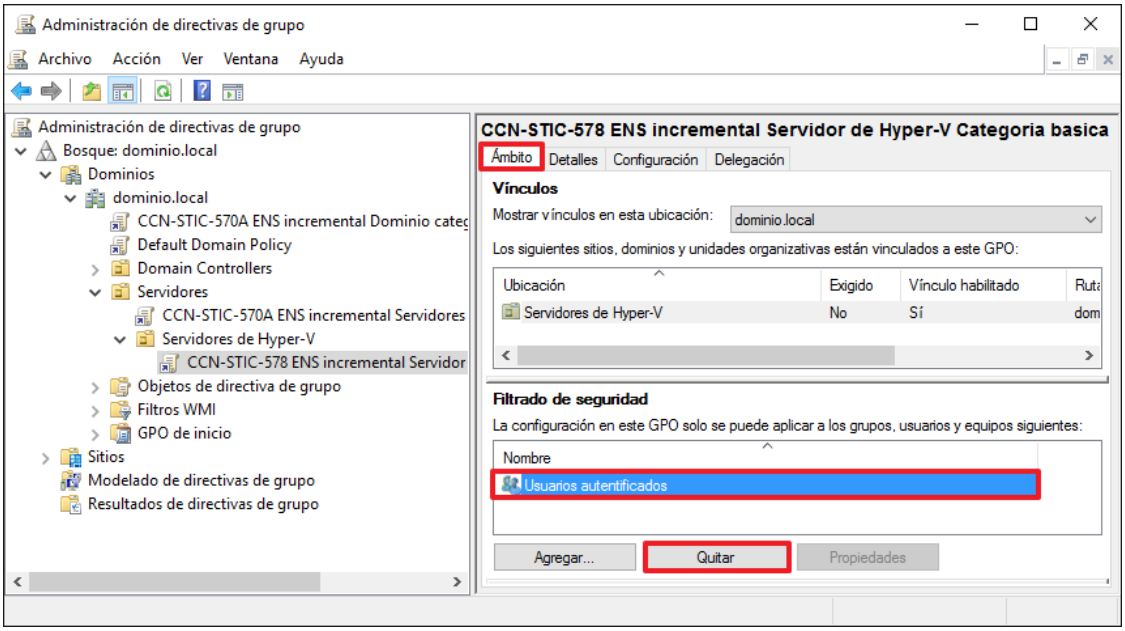
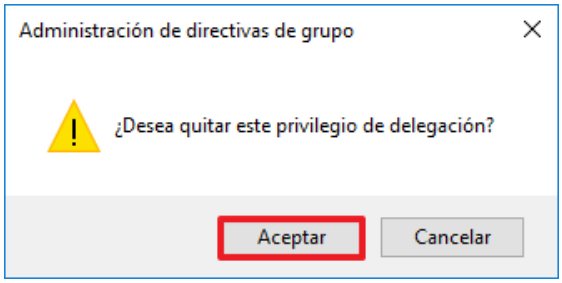
Paso	Descripción
11.	Inicie la herramienta “Usuarios y equipos Active Directory”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Usuarios y equipos de Active Directory”**. 
12.	En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo **“<<dominio>> → <<unidad organizativa>>”**, y desplegando el menú contextual con el botón derecho, seleccione la opción **“Nuevo → Unidad organizativa”**.  **Nota:** En este ejemplo, la unidad organizativa de servidores se encuentra en el nodo **“dominio.local → Servidores”**.

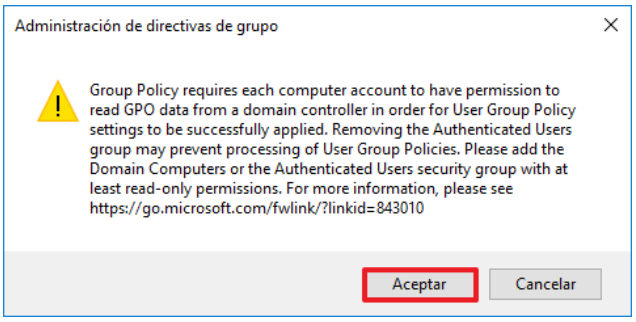
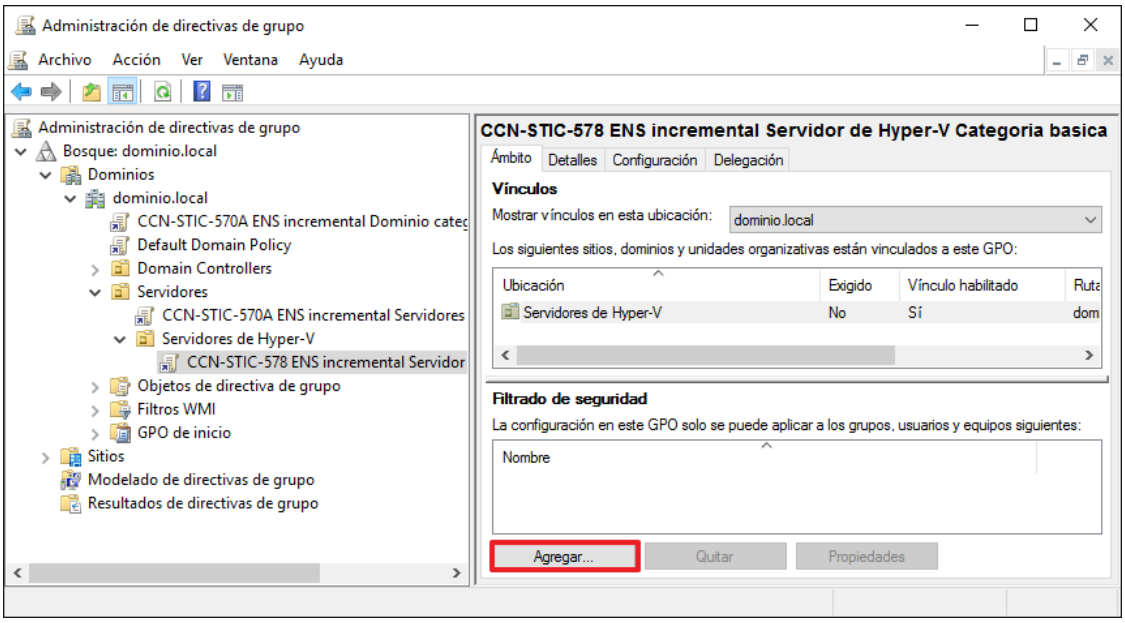
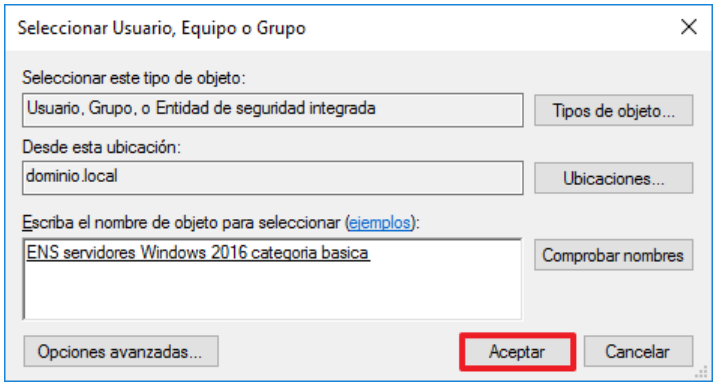
Paso	Descripción
13.	Introduzca el nombre “Servidores de Hyper-V” tal y como se muestra en la imagen y pulse sobre “Aceptar”. 
14.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores de virtualización a la unidad organizativa “Servidores de Hyper-V”. Para ello, haga clic con el botón derecho sobre el equipo que desee reubicar y seleccione la opción del menú contextual “Mover...”. 

Paso	Descripción
15.	A continuación, seleccione la unidad organizativa “Servidores de Hyper-V” y pulse “Aceptar”. 
16.	Cierre la herramienta “Usuarios y equipos de Active Directory”.
17.	A continuación, deberá crear la GPO "CCN-STIC-578 ENS incremental Servidor de Hyper-V categoria basica". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 
18.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
19.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administración de directivas de grupo”.** 

Paso	Descripción
20.	A continuación, despliegue el nodo **"Bosque: <<nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores de Hyper-V"**. **Nota:** En este ejemplo el nombre de la unidad organizativa donde se encuentran todos los servidores que implementan este rol, "Servidores de Hyper-V".
21.	Pulse con el botón derecho sobre la unidad organizativa "Servidores de Hyper-V" y seleccione "Crear un GPO en este dominio y vincularlo aquí…". 
22.	Introduzca el nombre del objeto GPO, "CCN-STIC-578 ENS incremental Servidor de Hyper-V Categoria basica" y haga clic en el botón "Aceptar". 

Paso	Descripción
23.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción "Editar". 
24.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad"**.
25.	Pulse con el botón derecho sobre "Configuración de seguridad" y seleccione la opción "Importar directiva…". 

Paso	Descripción
26.	Seleccione de la ruta "C:\Windows\Security\Templates" el fichero "CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria basica.inf" y pulse el botón "Abrir". 
27.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
28.	Seleccione la nueva política de grupo configurada y vaya a la pestaña "Ámbito" que se encuentra en el panel derecho. En la opción "Filtrado de seguridad", seleccione "Usuarios autentificados" y pulse la opción "Quitar". 
29.	Pulse "Aceptar" ante el mensaje emergente "¿Desea quitar este privilegio de delegación?". 

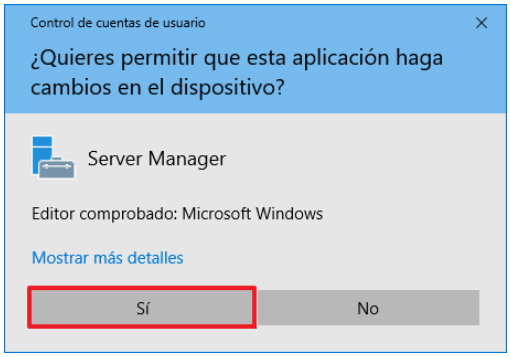
Paso	Descripción
30.	Pulse de nuevo “Aceptar” ante el mensaje de advertencia emergente. 
31.	A continuación, pulse el botón “Agregar…”. 
32.	Introduzca como nombre “ENS Servidores Windows 2016 categoria basica”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A Implementación del ENS en Windows Server 2016”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado, deberá adaptar estos pasos a las necesidades de su organización.

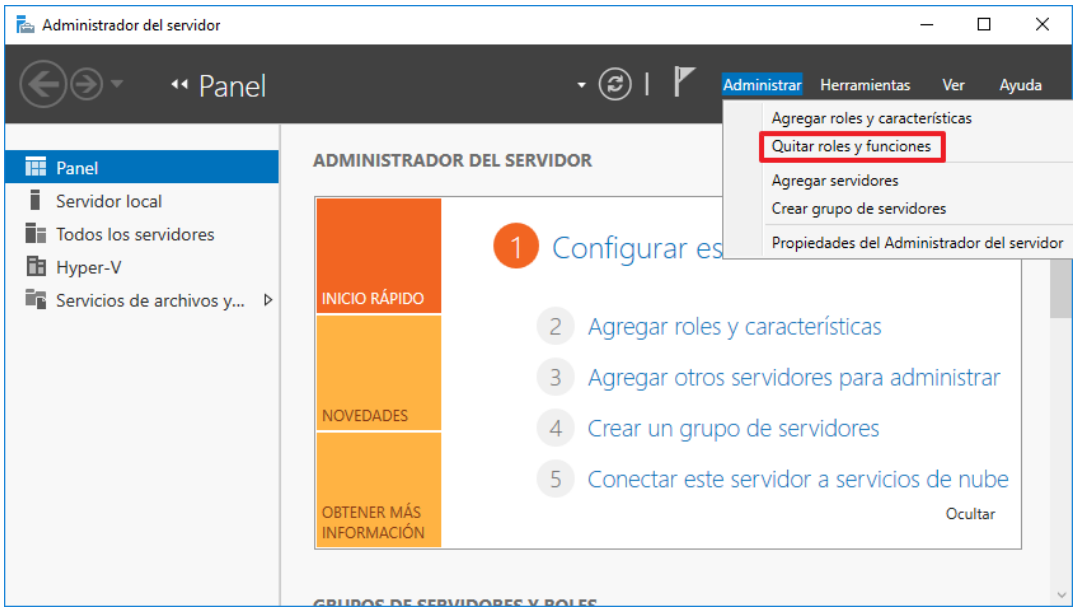
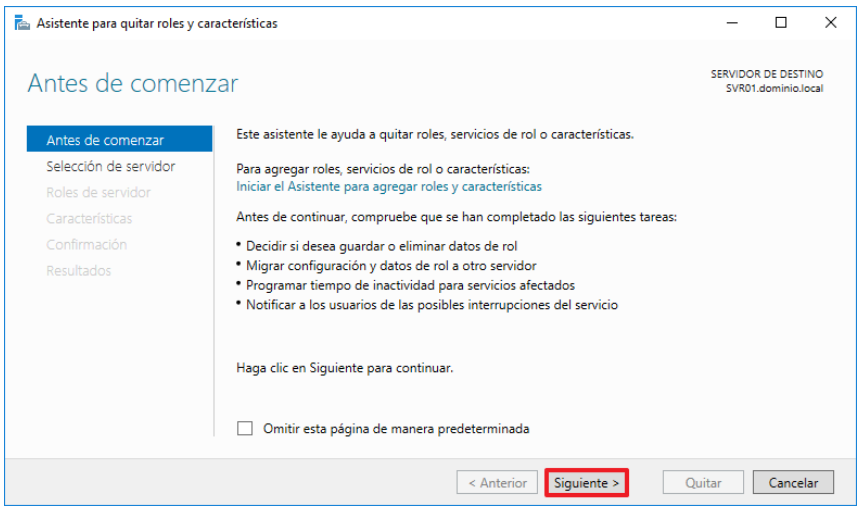
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

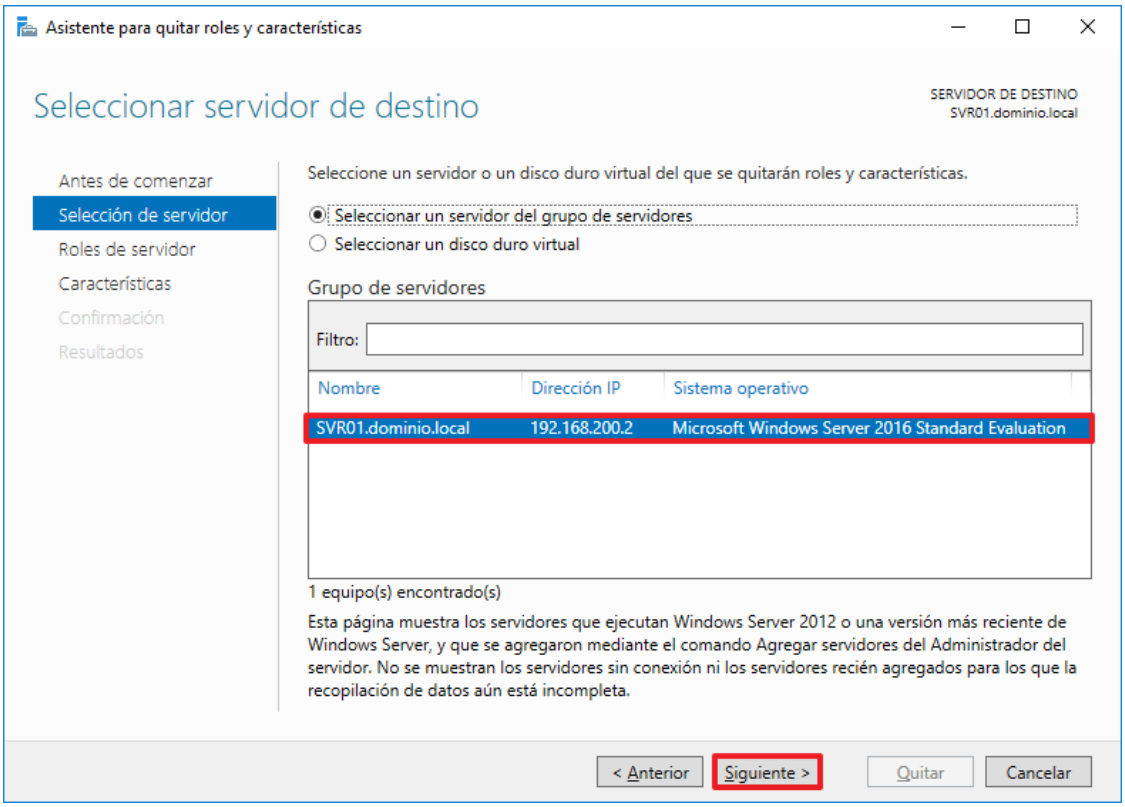
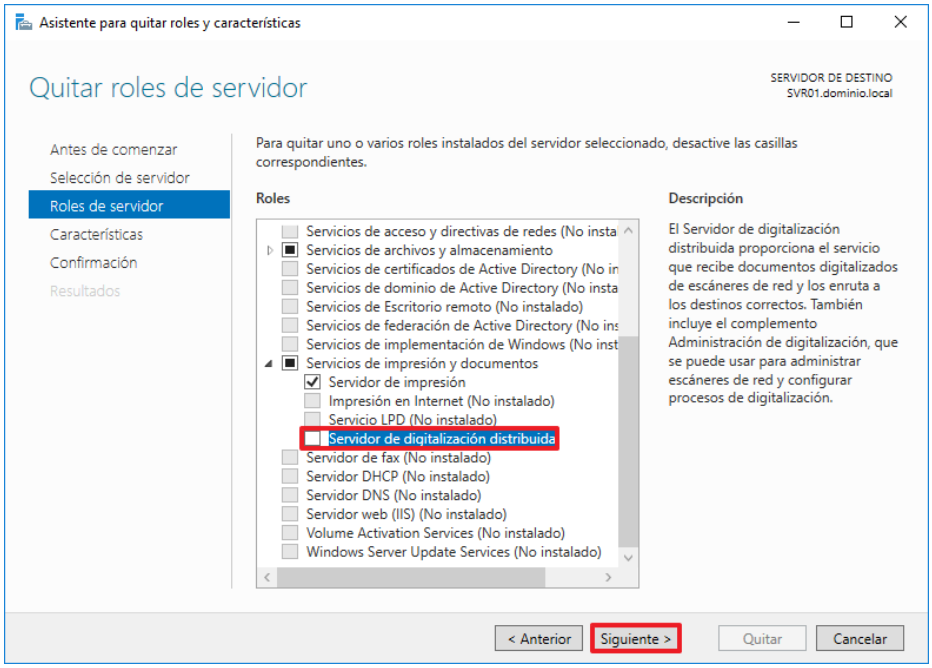
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

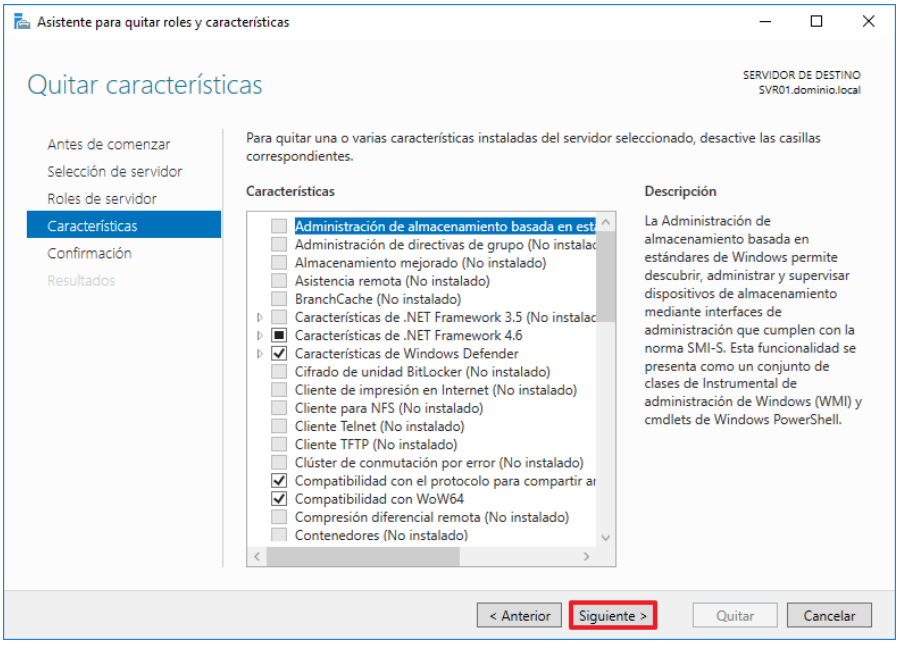
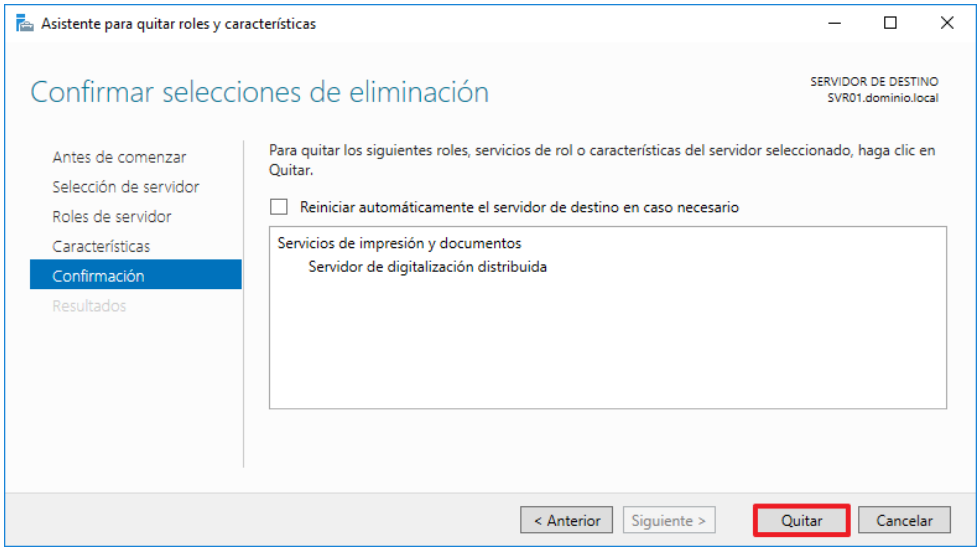
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

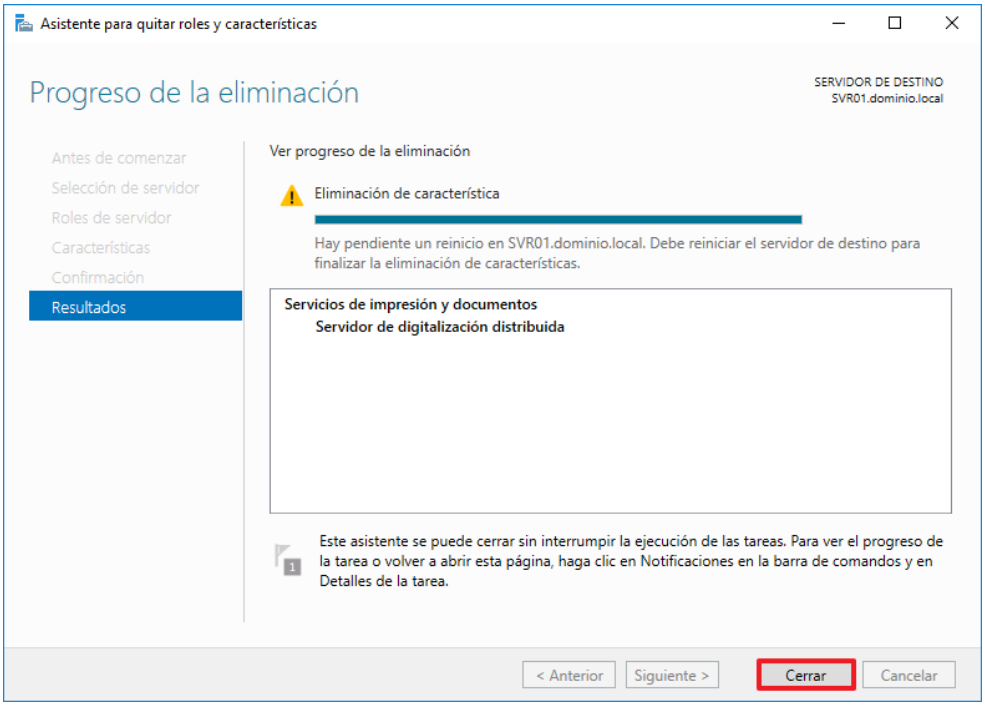
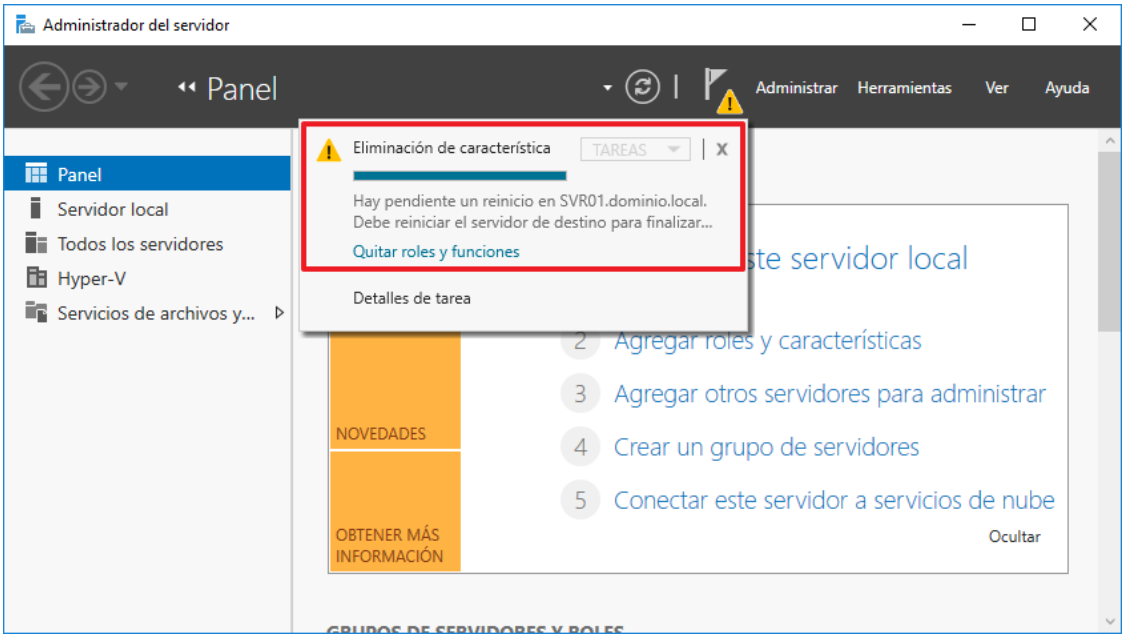
En el procedimiento que se describe a continuación, a modo de ejemplo, desinstala un rol que actualmente no está siendo utilizado por el Servidor de Hyper-V.

Paso	Descripción
33.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
34.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
35.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 

Paso	Descripción
36.	A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”. 
37.	Se lanzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 

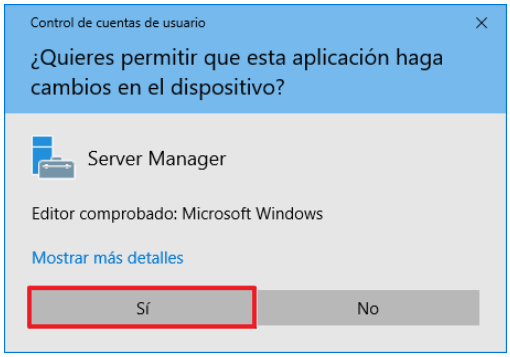
Paso	Descripción
38.	Seleccione el servidor sobre el cual desea eliminar un rol o característica y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “SVR01”.
39.	En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se desinstala el rol “Servidor de digitalización distribuida”.

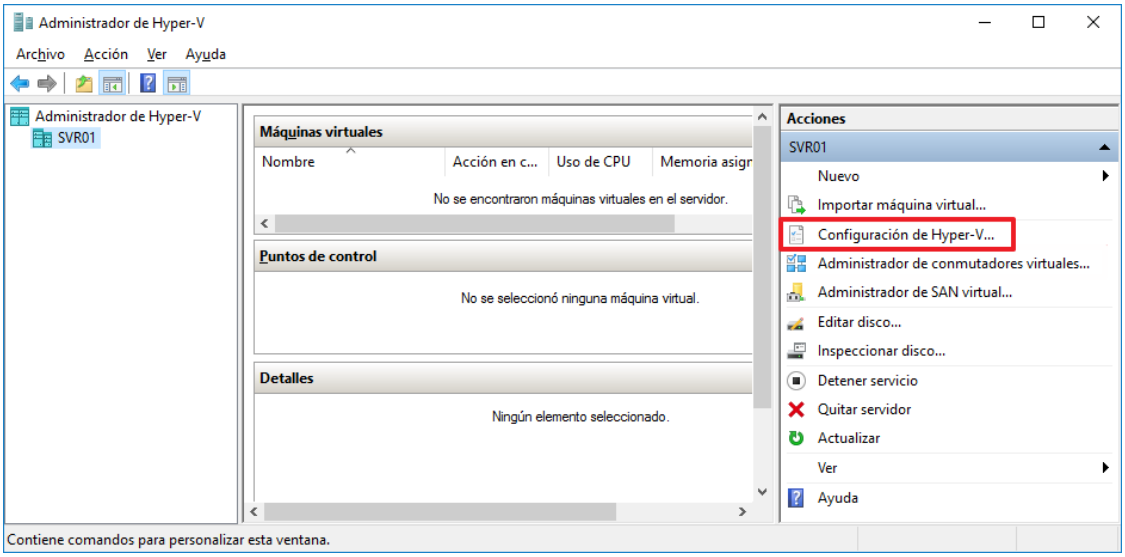
Paso	Descripción
40.	En la ventana de características pulse el botón “Siguiente >”. En este ejemplo no se desinstala ninguna característica adicional. 
41.	En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso. 

Paso	Descripción
42.	El proceso comenzará y una vez finalizado, y si todo ha ido bien bastará con pulsar sobre “Cerrar” para finalizar la desinstalación. 
43.	En caso de ser necesario el servidor requerirá un reinicio para finalizar la configuración. El “Administrador del servidor” mostrará una advertencia acerca de la necesidad de dicho reinicio. 

2.2. CONFIGURACIÓN GENERAL DE HYPER-V

La gestión de la configuración de Hyper-V constituye una importante tarea de administración debido a que permite establecer o modificar configuraciones que afectan a la funcionalidad del servicio de virtualización

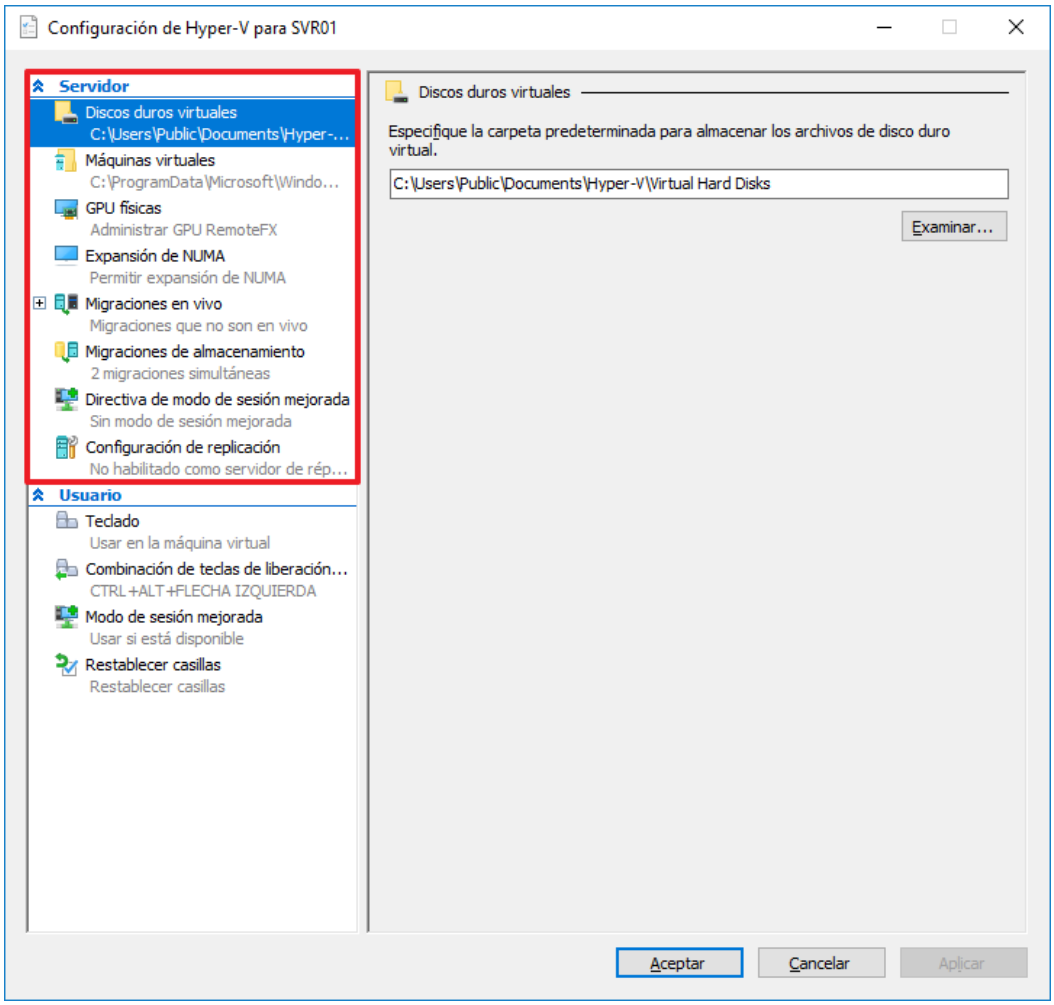
Paso	Descripción
44.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
45.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
46.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
47.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 

Paso	Descripción
48.	Dentro de la consola emergente seleccione el servidor de Hyper-V instalado en el servidor y a continuación en el panel de “Acciones” seleccione la opción “Configuración de Hyper-V…”. 
49.	En los siguientes apartados se definirán las configuraciones dedicadas al propio servidor de Hyper-V y aquellas configuraciones que afectan a la experiencia de usuario con el servicio de virtualización.

2.2.1. CONFIGURACIÓN DEL SERVIDOR

Este apartado define la configuración dedicada al servidor de Hyper-V la cual permite gestionar y administras las configuraciones más generales del servicio de virtualización.

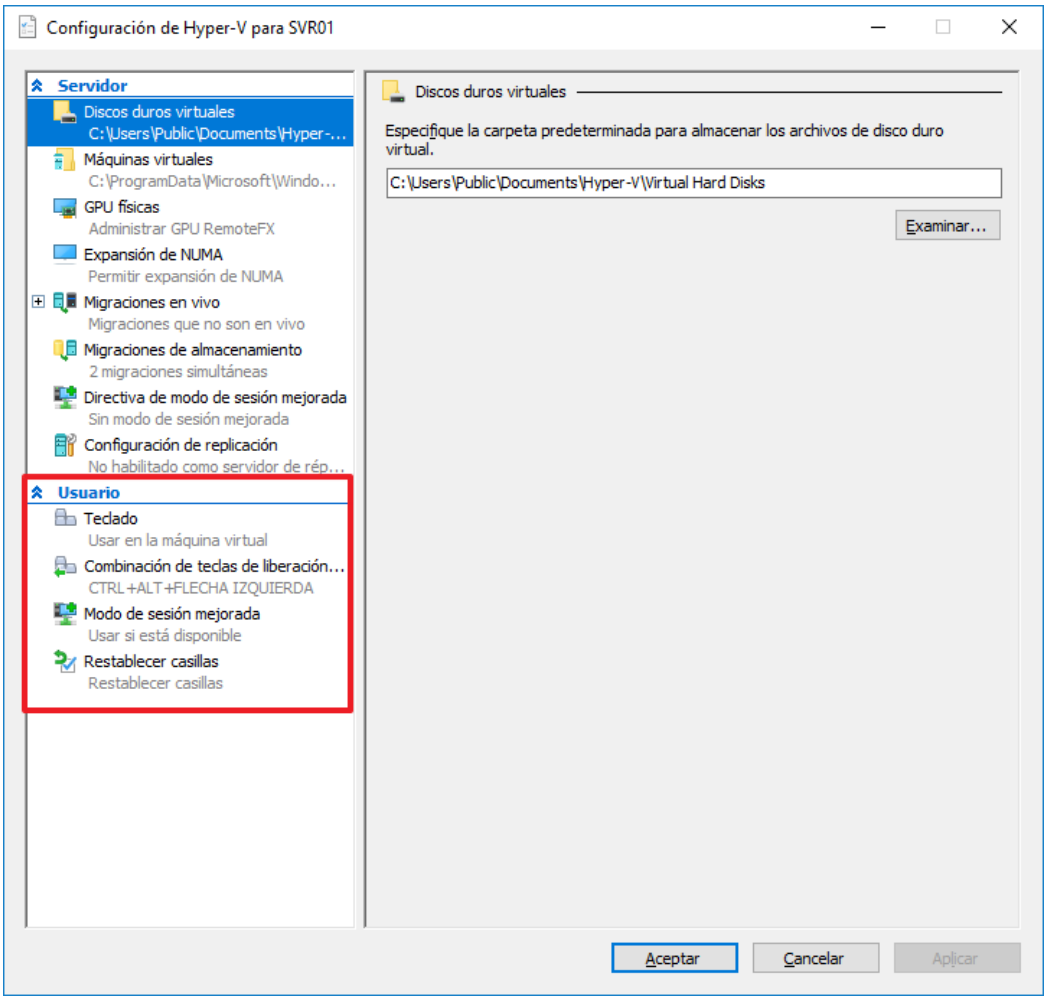
Paso	Descripción
50.	Dentro de la ventana “Configuración de Hyper-V para <<su servidor>>” acceda al apartado denominado “Servidor”.

Paso	Descripción
51.	Dentro de este apartado defina las configuraciones necesarias que permitan mejorar o establecer configuraciones de uso para el servidor Hyper-V 
52.	Dentro de estas configuraciones que es posible deberá prestar especial atención a las siguientes: – **Discos duros virtuales:** permite definir la ubicación por defecto de los discos de las máquinas virtuales. – **Máquinas virtuales:** permite definir la ubicación por defecto de los ficheros que componen las máquinas virtuales. – **Migraciones en vivo:** permite realizar migraciones de máquinas virtuales mientras éstas se encuentran en uso. – **Configuración de replicación:** esta configuración permite disponer de una copia casi instantánea en otro servidor de Hyper-V.

2.2.2. CONFIGURACIÓN DEL USUARIO

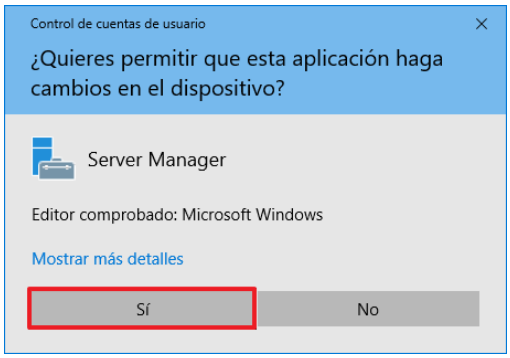
Este apartado define la configuración dedicada al usuario en su interacción con el servicio de virtualización.

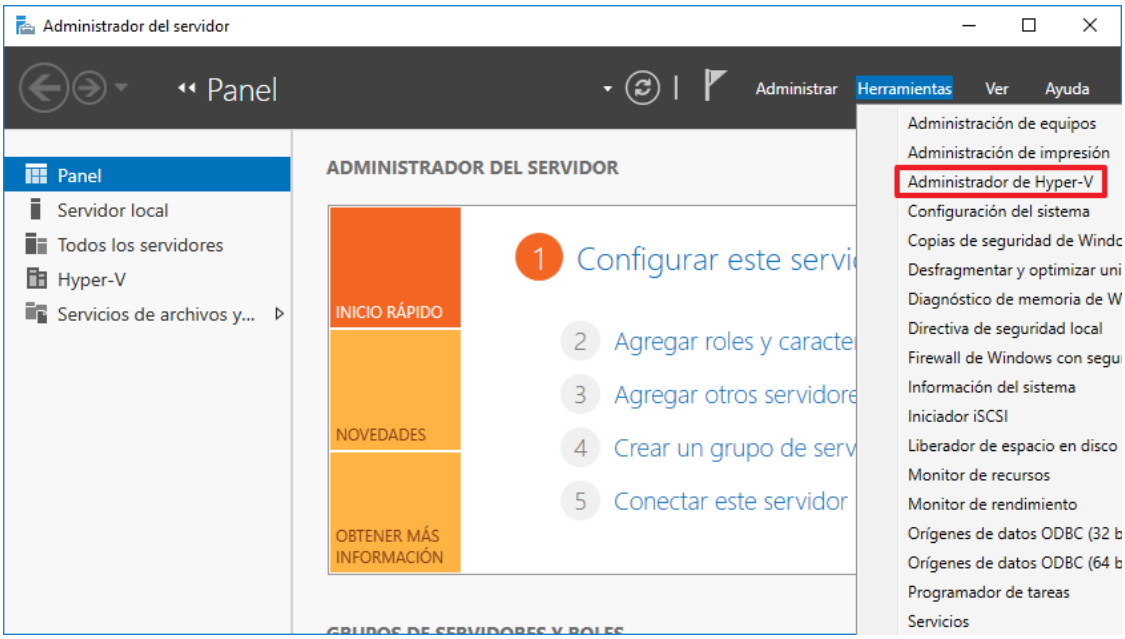
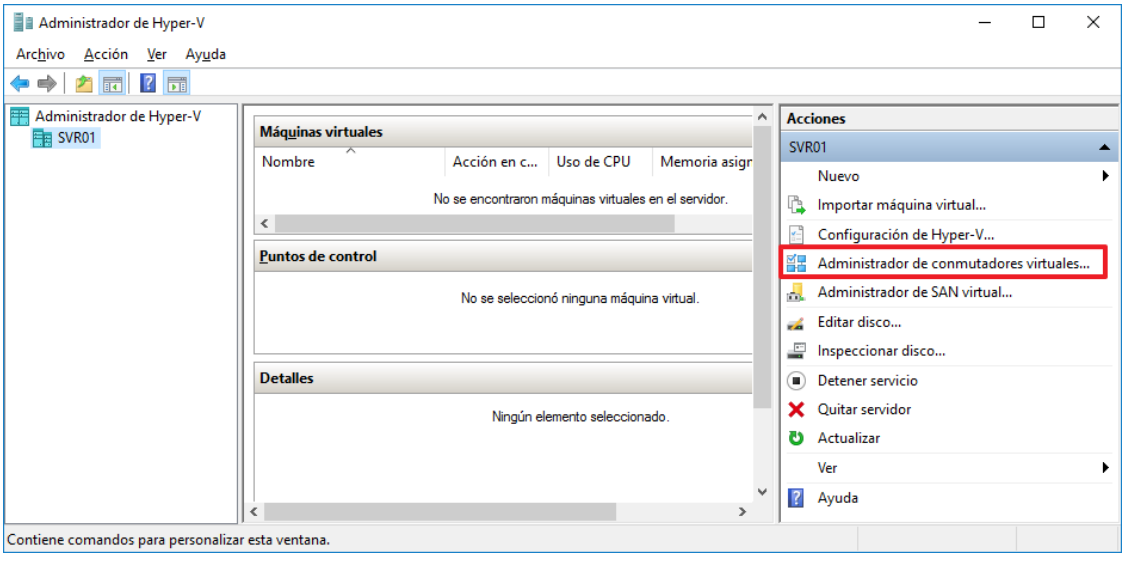
Paso	Descripción
53.	Dentro de la ventana “Configuración de Hyper-V para <<su servidor>>” acceda al apartado denominado “Usuario”.

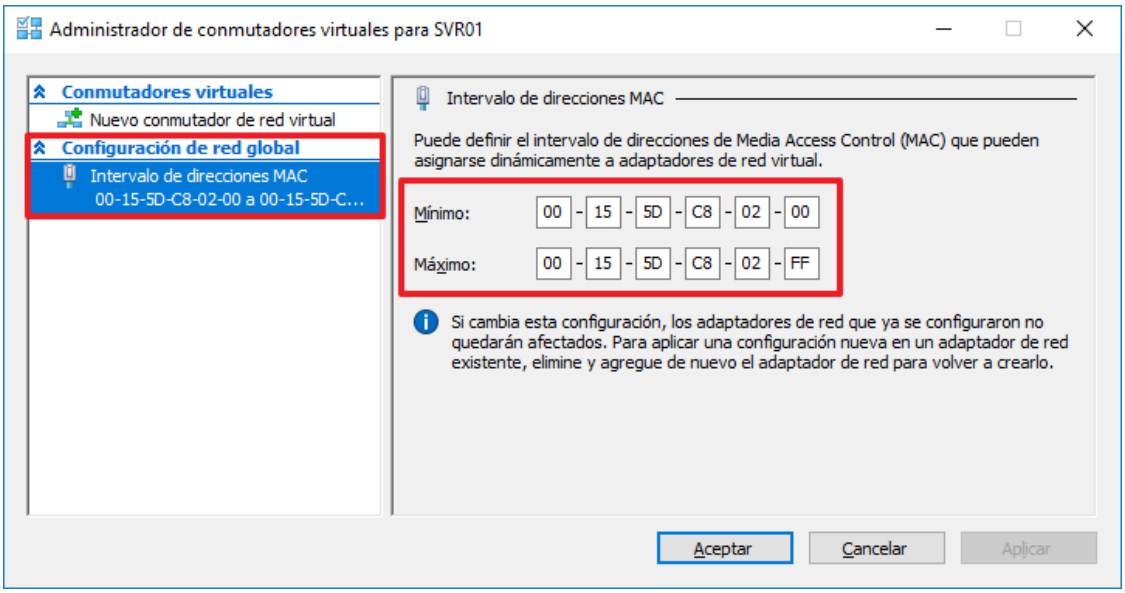
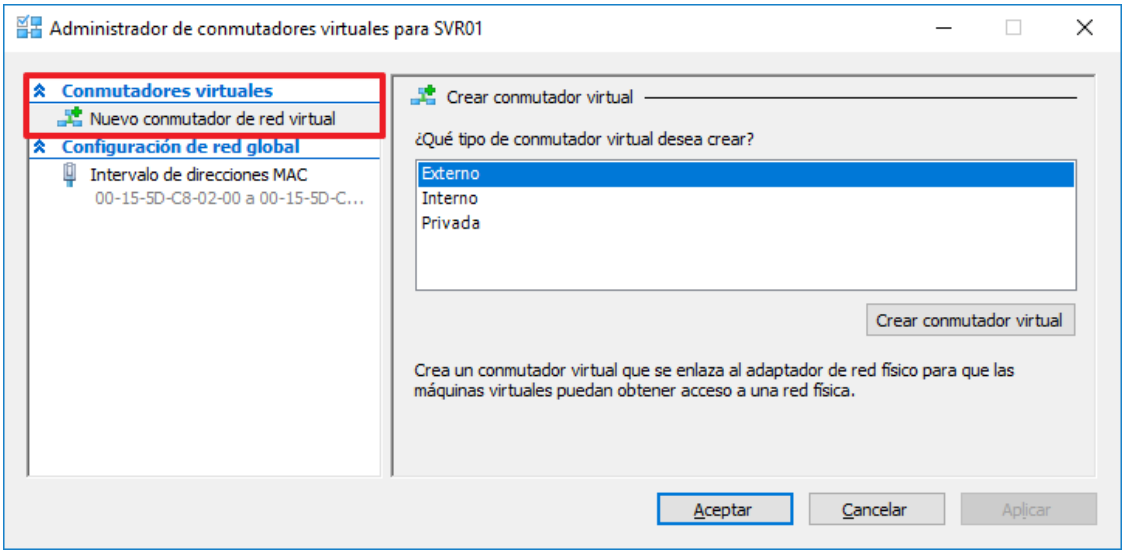
Paso	Descripción
54.	Dentro de este apartado defina las configuraciones necesarias que permitan mejorar o establecer configuraciones de uso para el servidor Hyper-V 
55.	Las configuraciones de las que dispone este apartado son las siguientes: – **Teclado:** permite establecer cómo se comportan las combinaciones de teclado en las máquinas virtuales. – **Combinación de teclas de liberación del mouse:** define la combinación de teclas a utilizar para “liberar” el ratón de la máquina virtual sobre la que se está trabajando. – **Modo de sesión mejorada:** permite el redireccionamiento de dispositivos y recursos locales (copiar y pegar) de equipos que ejecutan una conexión con una máquina virtual. – **Reestablecer casillas:** permite volver a un estado de “recién instalado” en el que Hyper-V muestra mensajes de confirmación que han sido ya omitidos.

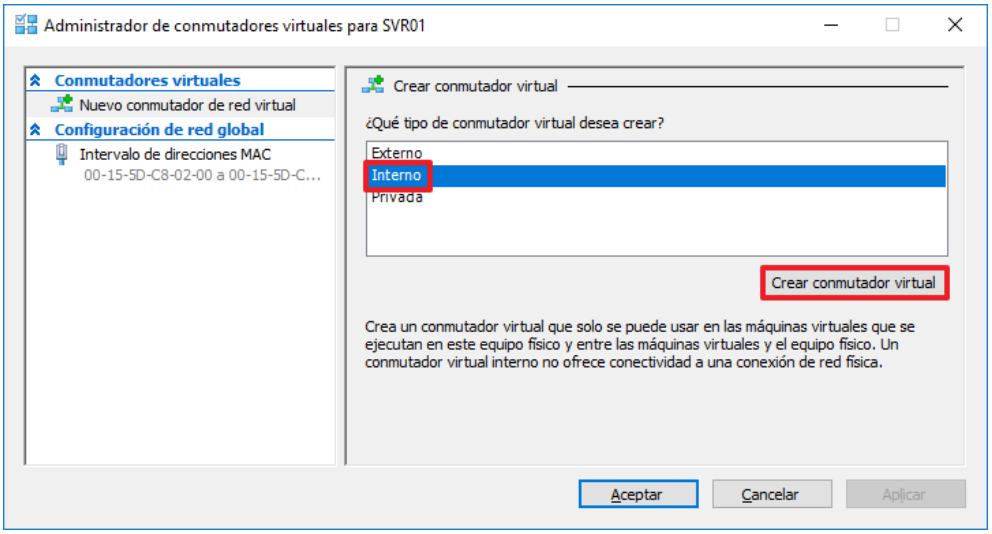
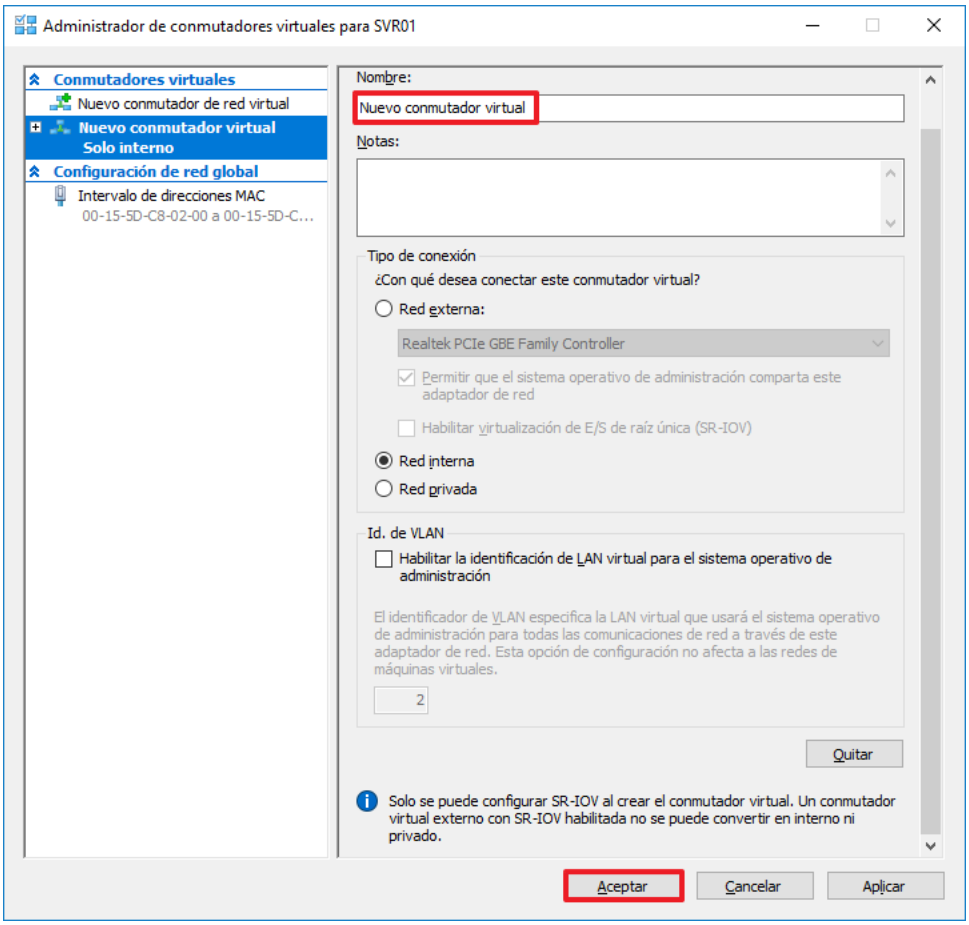
2.3. GESTIÓN DE CONMUTADORES VIRTUALES

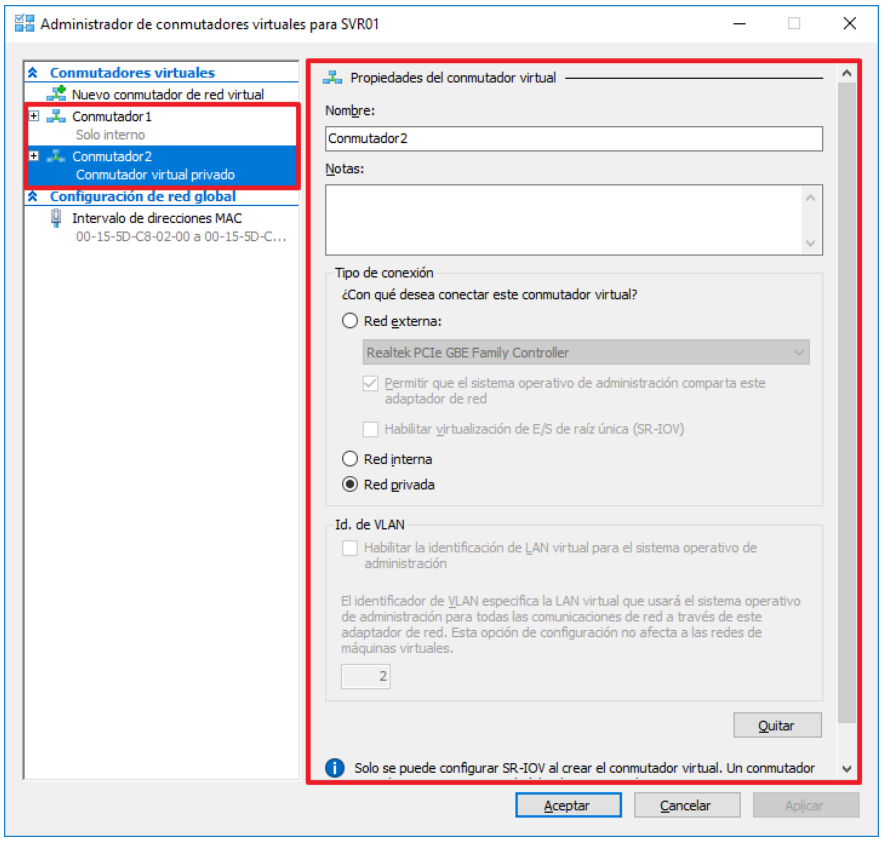
Dentro del servidor de Hyper-V es importante realizar una correcta gestión de las redes disponibles con el fin de determinar cómo se comporta la red de las diferentes máquinas virtuales y permitir establecer o denegar comunicaciones según sea necesario.

Paso	Descripción
56.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
57.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
58.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 

Paso	Descripción
59.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
60.	Dentro de la consola emergente seleccione el servidor de Hyper-V instalado en el servidor y a continuación en el panel de "Acciones" seleccione la opción "Administrador de conmutadores virtuales". 

Paso	Descripción
61.	En la ventana emergente “Administrador de conmutadores virtuales para <<su servidor>>” dentro del apartado “Configuración de red global” seleccione “Intervalo de direcciones MAC”. Establezca el intervalo mínimo y máximo de direcciones MAC que pueden asignarse a los adaptadores de red virtuales.  **Nota:** Deberá tener en cuenta las especificaciones necesarias para establecer el direccionamiento MAC adecuado. En este ejemplo, se establece por defecto.
62.	A continuación, seleccione dentro del apartado “Conmutadores virtuales” la opción “Nuevo conmutador de red virtual”. 

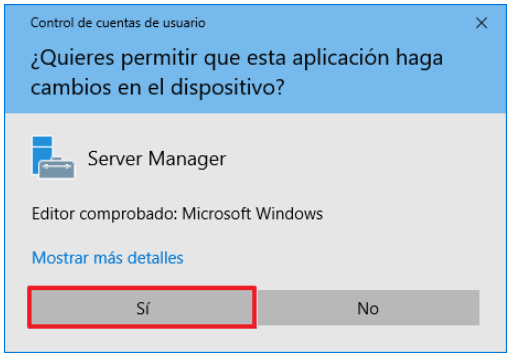
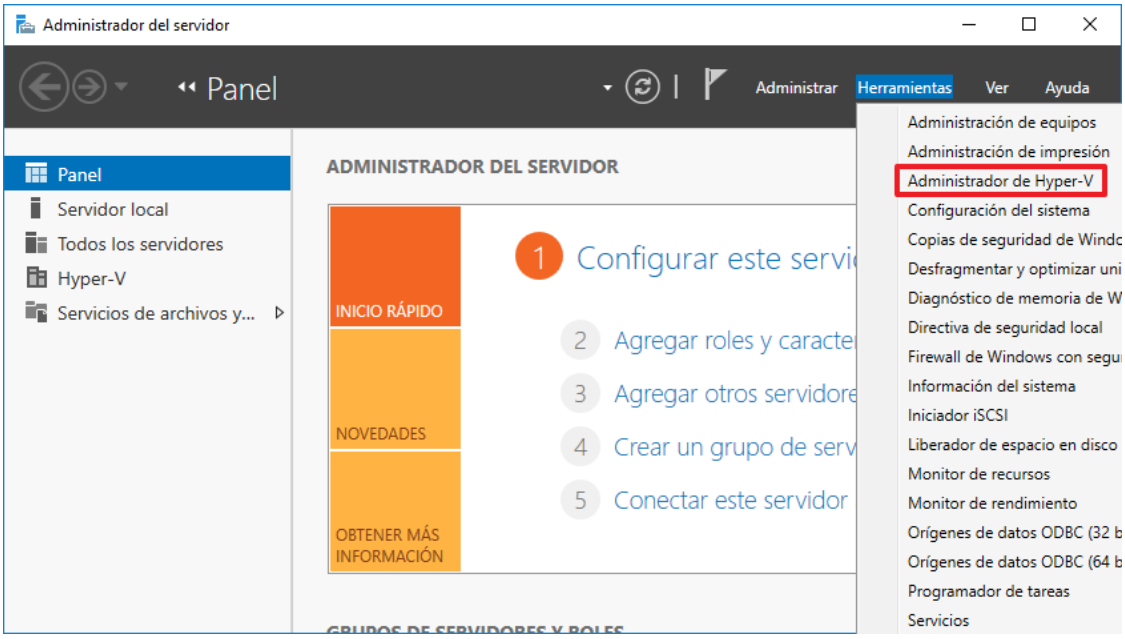
Paso	Descripción
63.	Seleccione entonces el tipo de conmutador virtual de red deseado. Deberá tener en consideración las necesidades de su organización en el momento de crear dichos adaptadores virtuales de red.  **Nota:** Para este ejemplo se crea un conmutador de red "Interno"
64.	Aparecerá otra ventana en la que se mostrarán las opciones disponibles sobre el adaptador de red creado. Establezca un nombre y si lo desea una descripción. Por último, pulse sobre "Aceptar". 

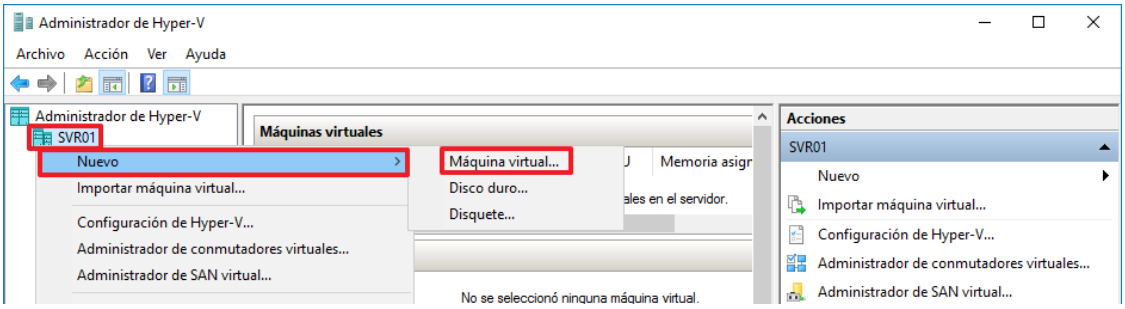
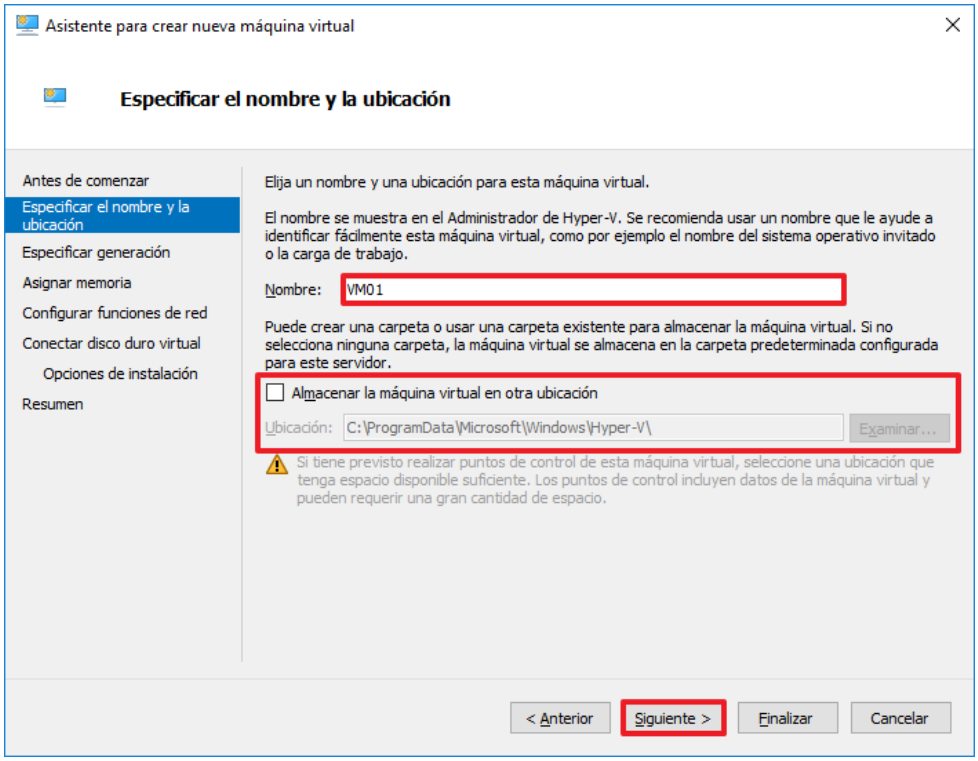
Paso	Descripción
65.	Podrá realizar una gestión sobre los conmutadores creados pulsando sobre cada uno de ellos y modificando la configuración que ya poseen. Del mismo modo es posible eliminar conmutadores que ya no sean requeridos haciendo uso del botón “Quitar”. 

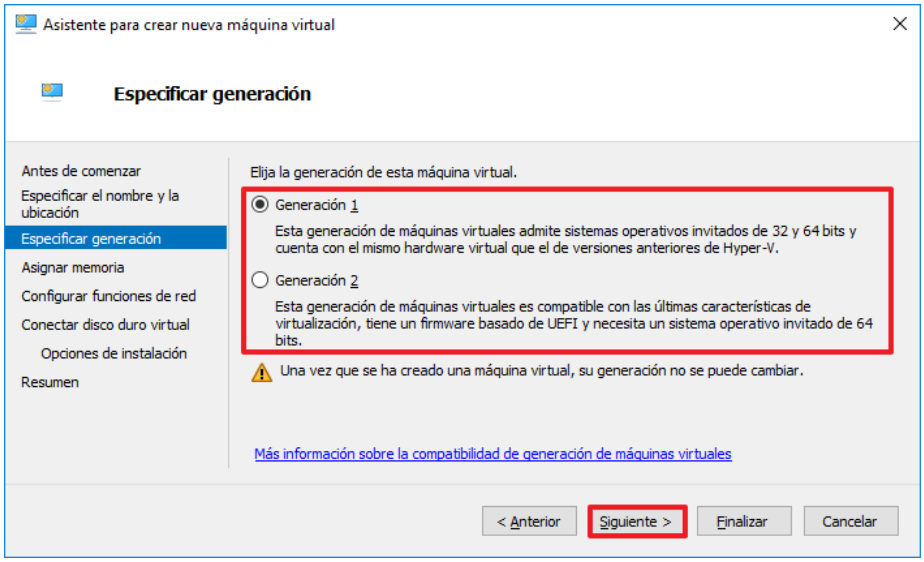
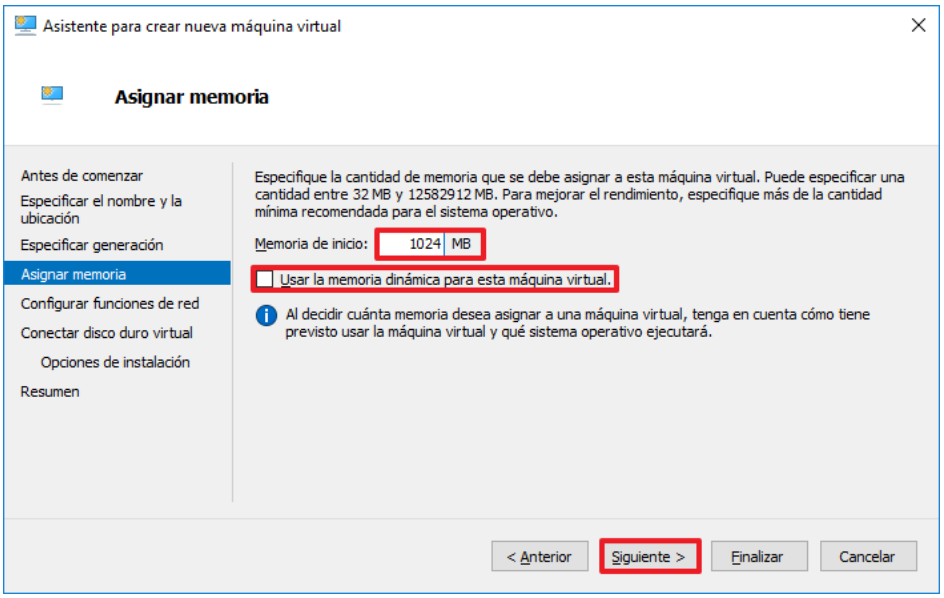
2.4. GESTIÓN DE MÁQUINAS VIRTUALES

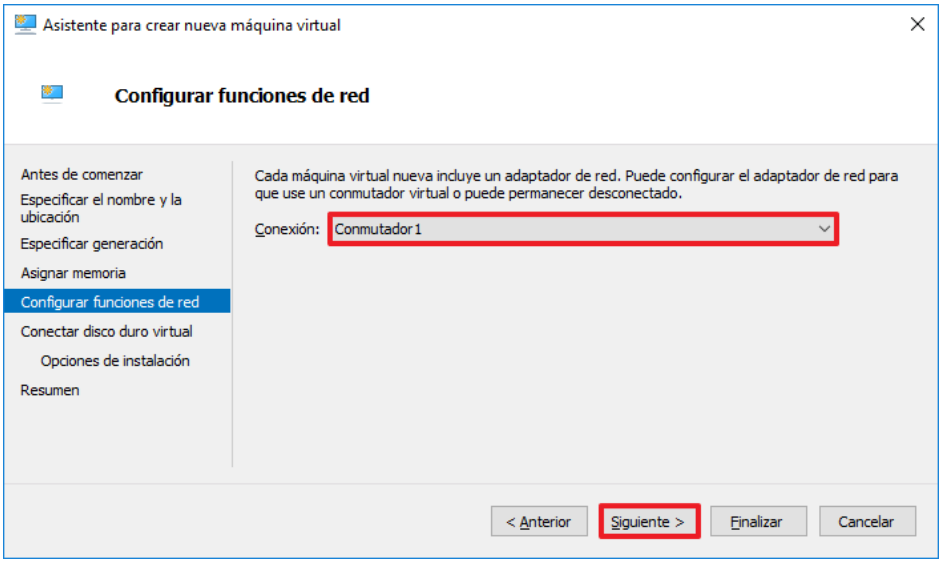
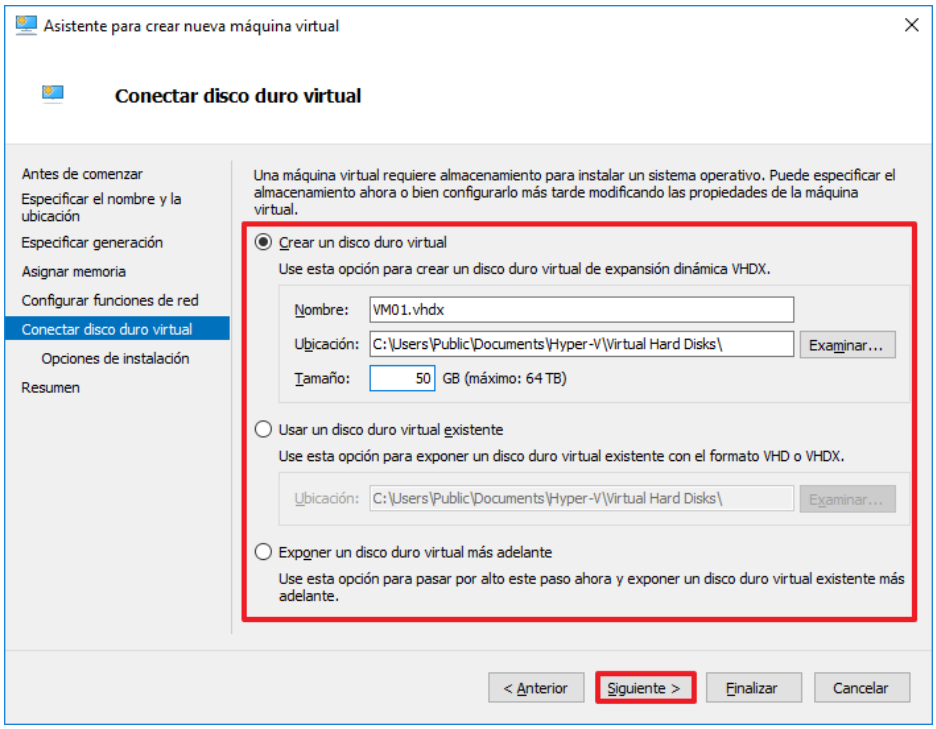
Otra de las tareas esenciales es la creación de máquinas virtuales ya que éstas son las que ofrecen el servicio propiamente dicho. En este apartado se realiza un ejemplo de creación y configuración de una máquina virtual.

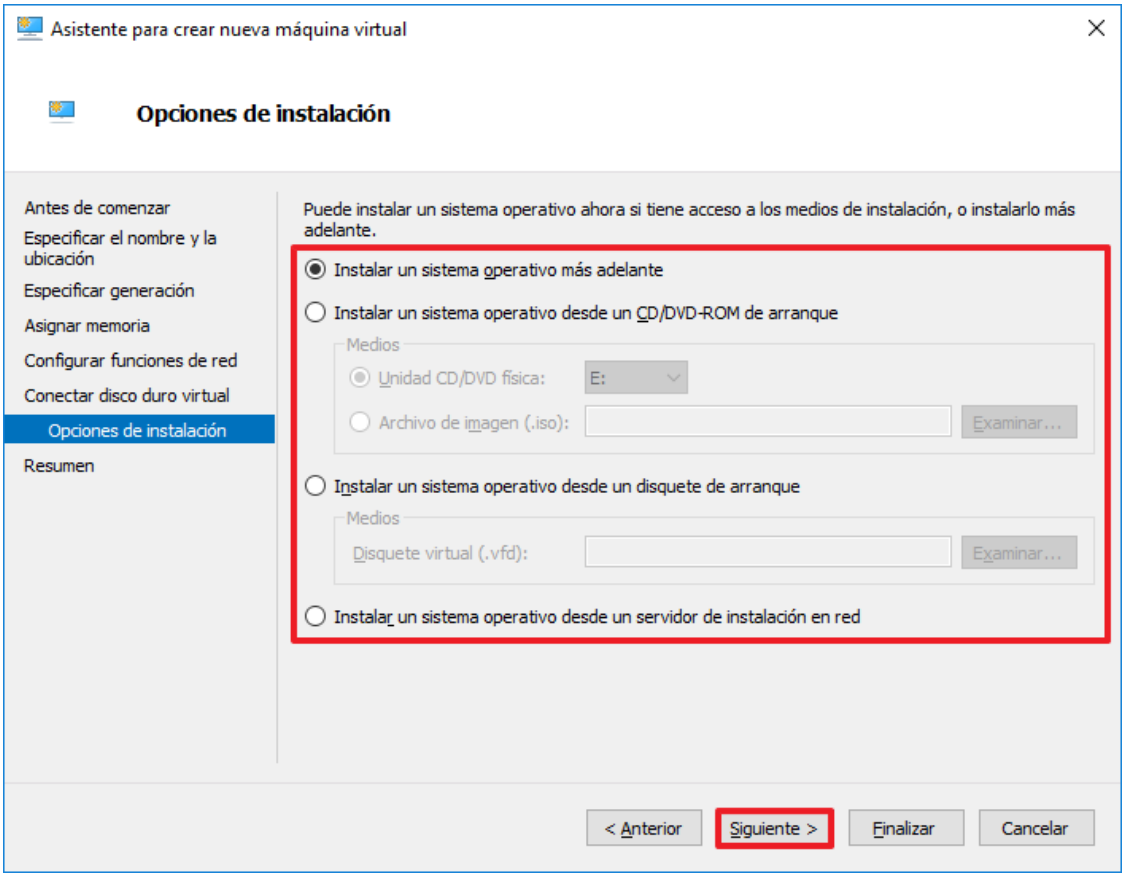
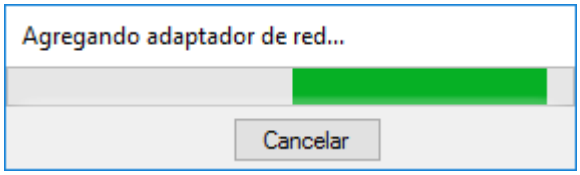
Paso	Descripción
66.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

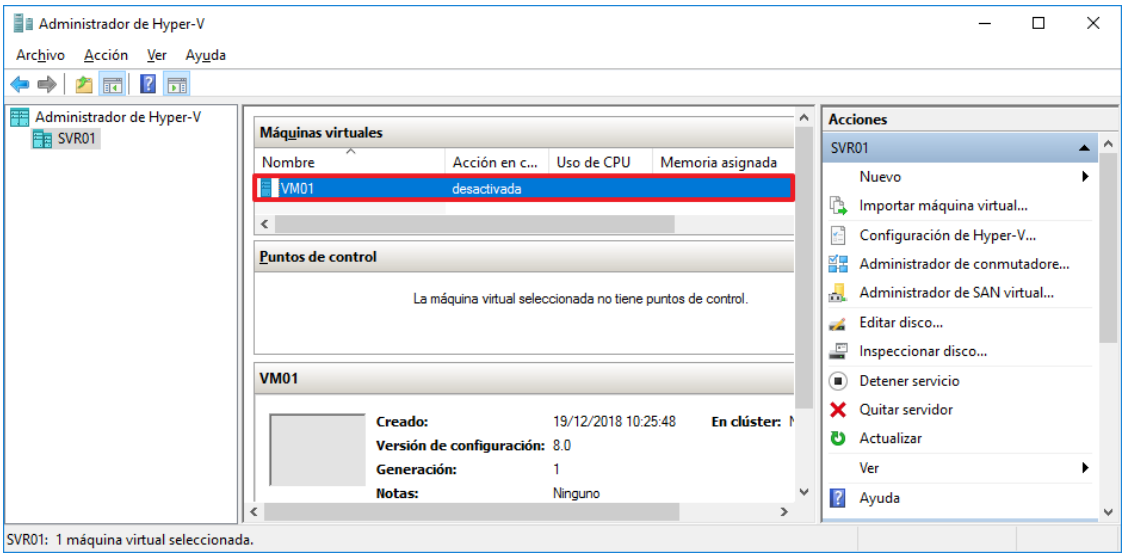
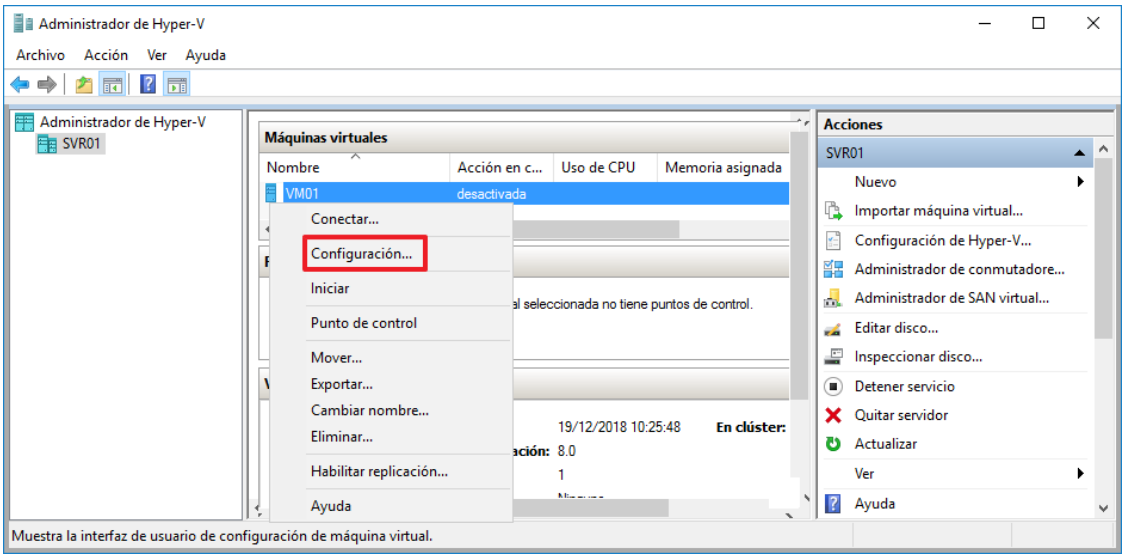
Paso	Descripción
67.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
68.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
69.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 

Paso	Descripción
70.	Dentro de la consola emergente seleccione el servidor de Hyper-V con el botón derecho y seleccione la opción del menú contextual **"Nuevo → Máquina virtual…"**.  **Nota:** En este ejemplo el servidor de denomina "SVR01". Deberá adaptar estos pasos a las configuraciones de su organización.
71.	Aparecerá el asistente para la creación de máquinas virtuales. En la ventana "Antes de comenzar" pulse "Siguiente >".
72.	En la ventana "Especificar el nombre y la ubicación" determine el nombre que poseerá la máquina dentro de Hyper-V y una ubicación concreta si lo desea. Pulse "Siguiente >" para continuar.  **Nota:** Tenga en consideración que si realizó alguna modificación en el apartado "2.2 CONFIGURACIÓN GENERAL DE HYPER-V" la ubicación por defecto ya deberá estar configurada a la requerida por su organización. En este ejemplo se crea la máquina "VM01", deberá adaptar los nombres a las necesidades de su organización".

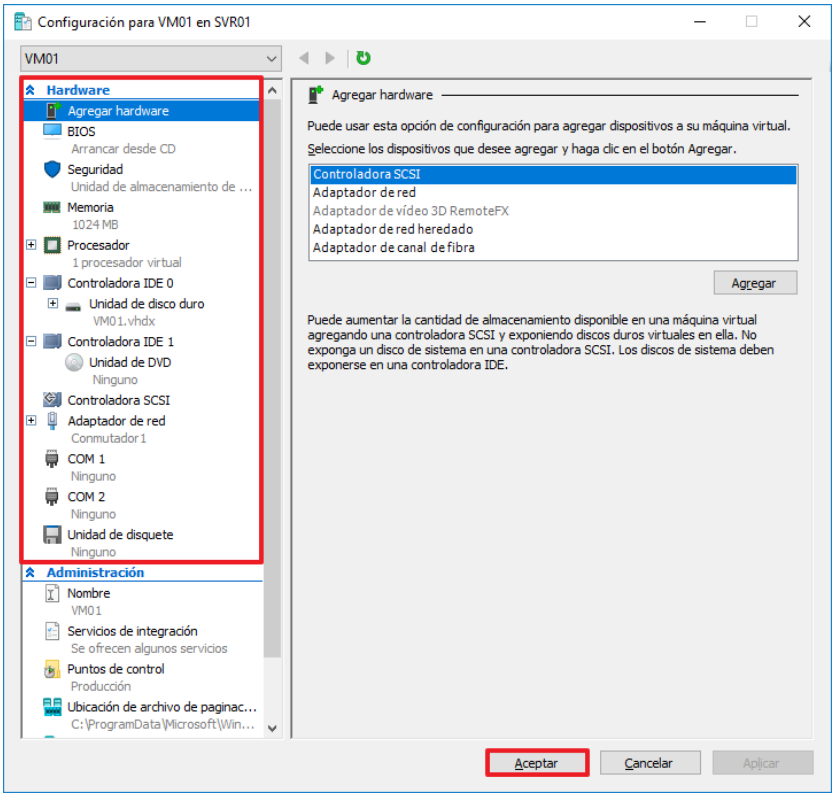
Paso	Descripción
73.	En la ventana “Especificar generación” deberá determinar la generación de las máquinas creadas. Esto afectará en las características de las mismas. Pulse “Siguiente >” cuando haya finalizado.  **Nota:** En este ejemplo se opta por marcar “Generación 1”. Esta configuración deberá adaptarse a las necesidades de su organización. Una vez creada la máquina esta configuración no puede modificarse. Tenga este hecho presente de cara a futuras configuraciones que puedan ser requeridas como el “ANEXO A.5.2 CIFRADO DE MÁQUINAS VIRTUALES”.
74.	En la ventana “Asignar memoria” deberá determinar la memoria RAM de la máquina virtual. Además, podrá establecer el uso de memoria RAM de forma dinámica si lo desea. Pulse “Siguiente >” para seguir con el asistente.  **Nota:** Dependiendo de los recursos y las especificaciones de la máquina a implementar deberá configurar este valor. En este ejemplo se asigna “1024 MB” de memoria RAM.

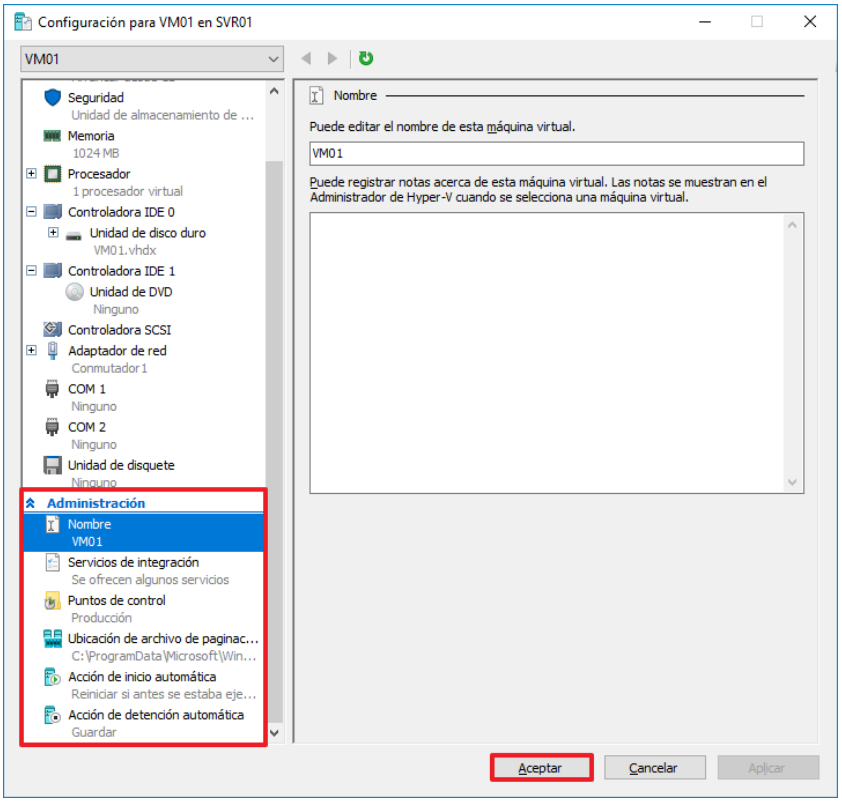
Paso	Descripción
75.	En la ventana “Configurar funciones de red” asigne uno de los conmutadores de los que disponga ya configurados. Pulse sobre el botón “Siguiente >” cuando finalice.  **Nota:** Deberá conectar el adaptador deseado en función de las necesidades de su organización. Esta configuración puede modificarse también tras crear la máquina. En este ejemplo se asigna el adaptador “Conmutador1”.
76.	En la ventana “Conectar disco duro virtual” cree un disco duro virtual nuevo, asigne uno ya creado u omita este paso para exponer el disco más adelante. Pulse “Siguiente >” para continuar.  **Nota:** En este ejemplo se crea un disco virtual vacío con 50 GB de tamaño. Adapte el tamaño y la configuración a las necesidades de su organización.

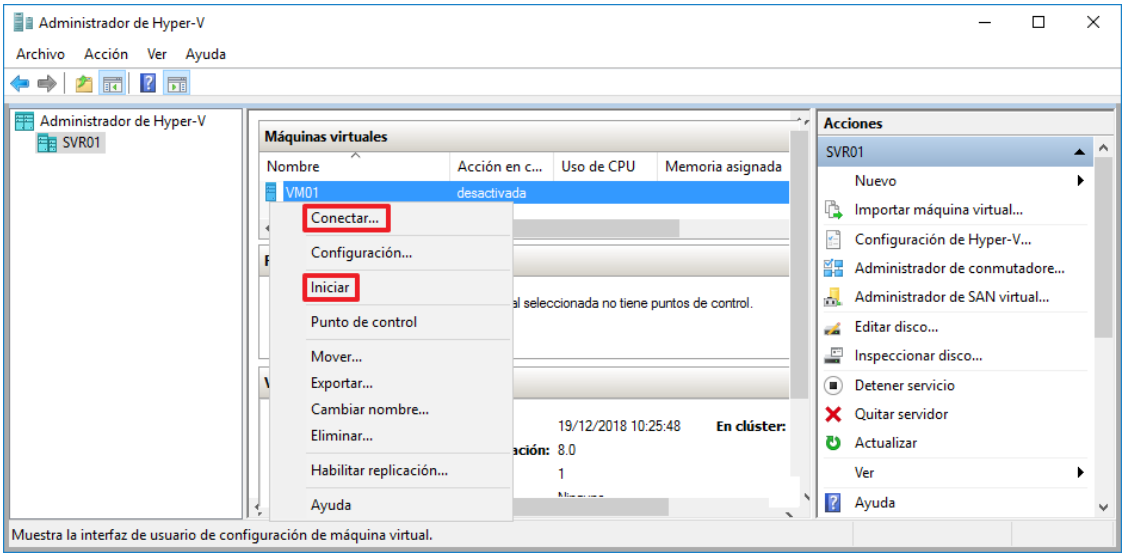
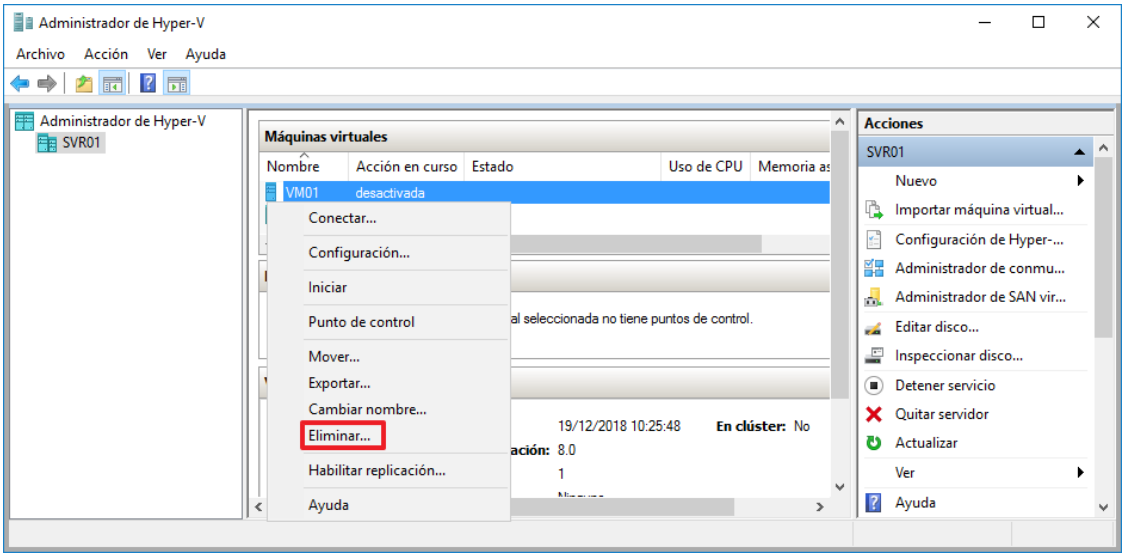
Paso	Descripción
77.	En la ventana “Opciones de instalación” configure un medio de arranque para la máquina virtual. Pulse “Siguiente >” cuando finalice.  **Nota:** En este ejemplo de opta por instalar un sistema operativo más adelante. Adapte este paso a las necesidades de su organización.
78.	Por último, en la ventana “Resumen” compruebe que las configuraciones de la máquina virtual son correctas. En caso afirmativo pulse “Finalizar”. Si por el contrario requiere modificar alguna configuración pulse el botón “< Anterior” hasta llegar a la ventana deseada y modifique la configuración.
79.	Comenzará el proceso de creación el cual podrá variar dependiendo de las especificaciones de la máquina virtual. 

Paso	Descripción
80.	Cuando haya finalizado la máquina virtual aparecerá en el panel central de “Administrador de Hyper-V”. 
81.	Para modificar la configuración establecida durante la creación o bien añadir más recursos haga clic derecho sobre la máquina deseada y pulse sobre la opción del menú contextual “Configuración…”. 

Paso	Descripción
82.	De mismo modo podrá realizar diferentes configuraciones que afectan al comportamiento de la máquina virtual y a la experiencia de usuario con dicha máquina. Pulse “Aceptar” cuando haya finalizado.

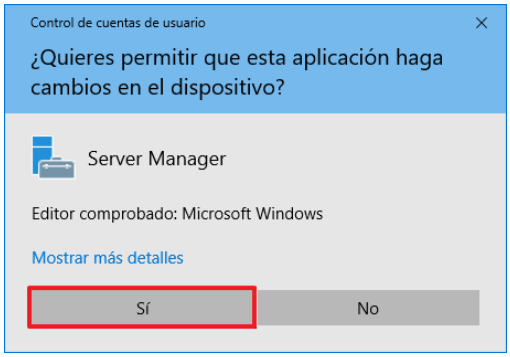


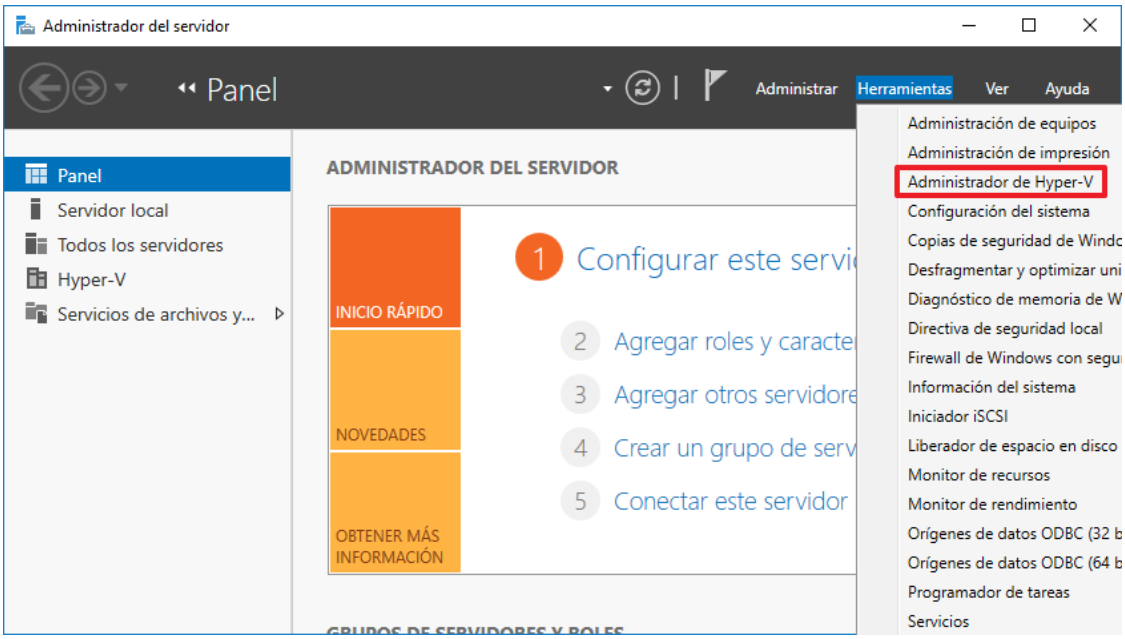
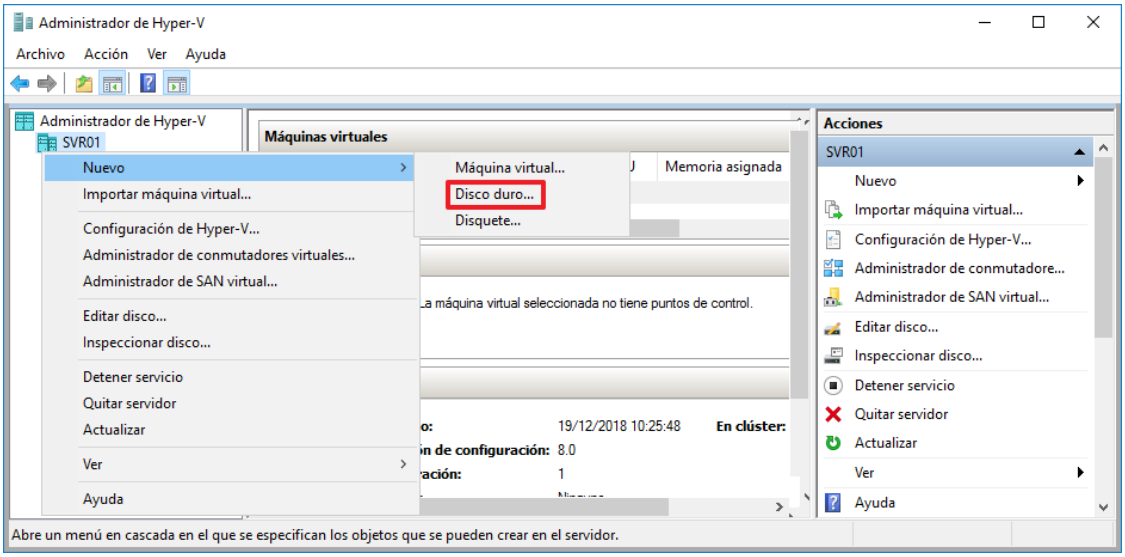


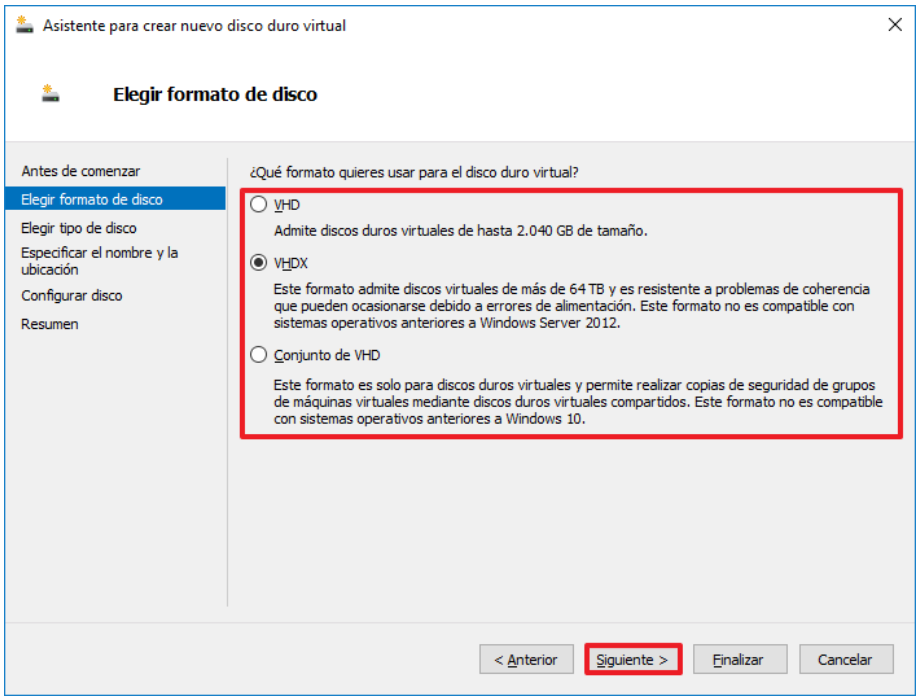
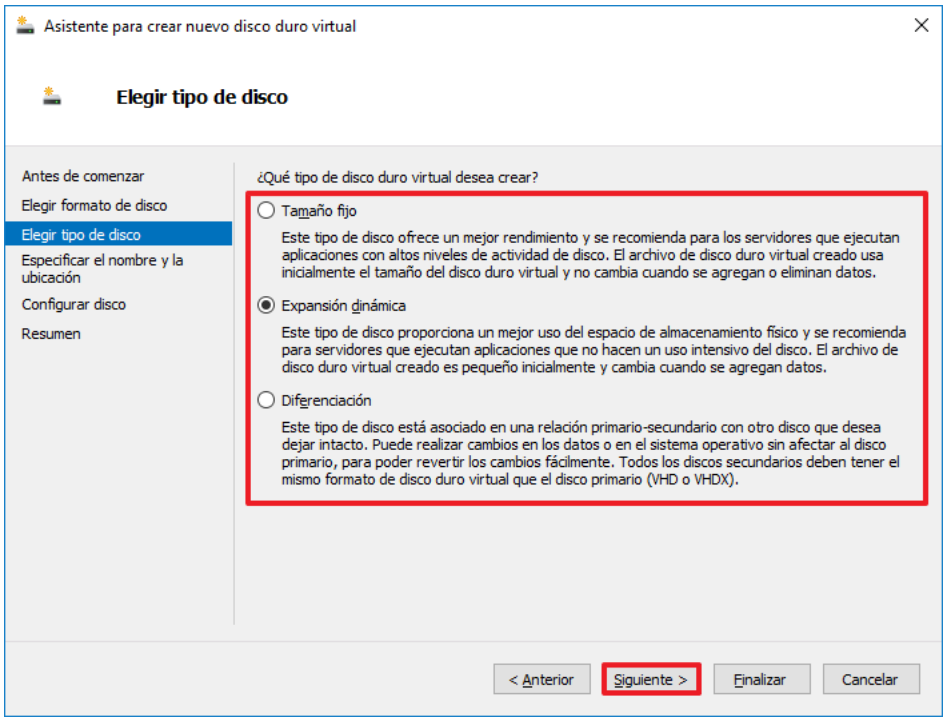
Paso	Descripción
83.	Por último, cuando la máquina esté finalizada podrá iniciarla y conectar con ella haciendo clic derecho y pulsando sobre las opciones del menú contextual “Iniciar” y “Conectar”, respectivamente. 
84.	En el caso de no disponer de disco virtual deberá consultar el apartado siguiente “2.5 GESTIÓN DE DISCOS DUROS VIRTUALES”.
85.	Si desea eliminar alguna de las máquinas haga clic derecho sobre ella y seleccione la opción del menú contextual “Eliminar…”.  **Nota:** Tenga en consideración que la eliminación de los discos asociados a la máquina deberá realizarse de forma manual.

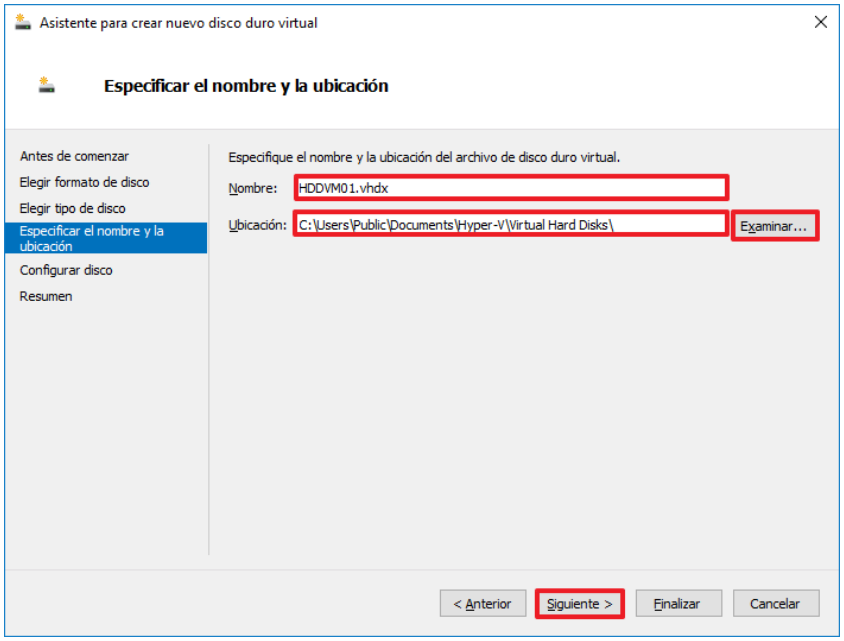
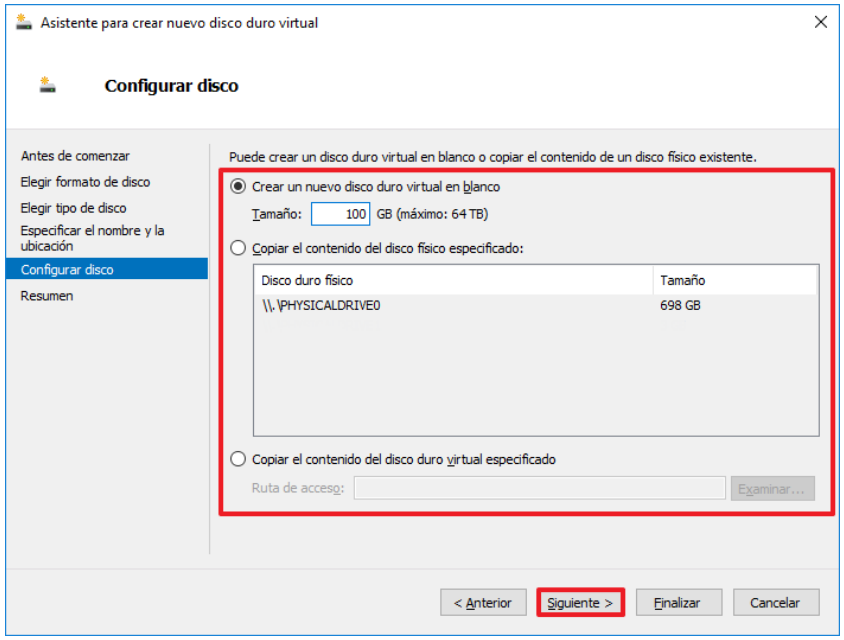
2.5. GESTIÓN DE DISCOS DUROS VIRTUALES

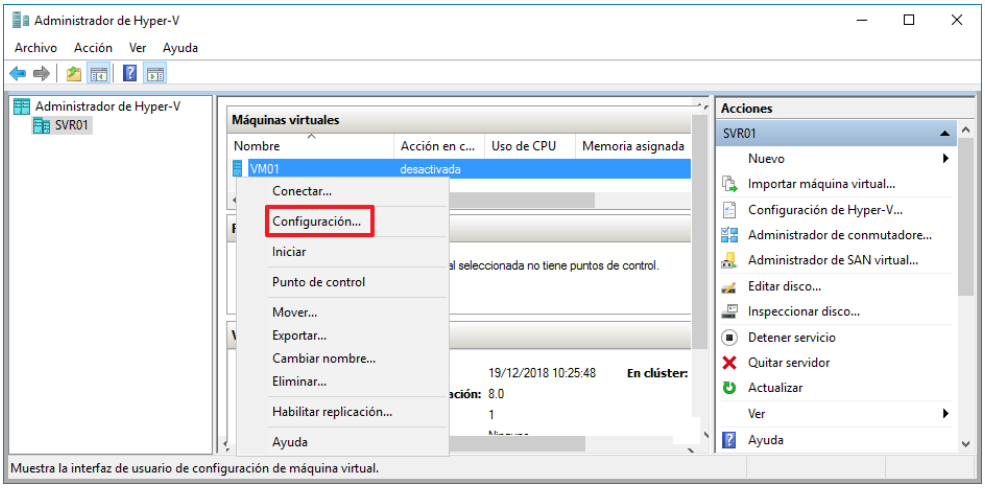
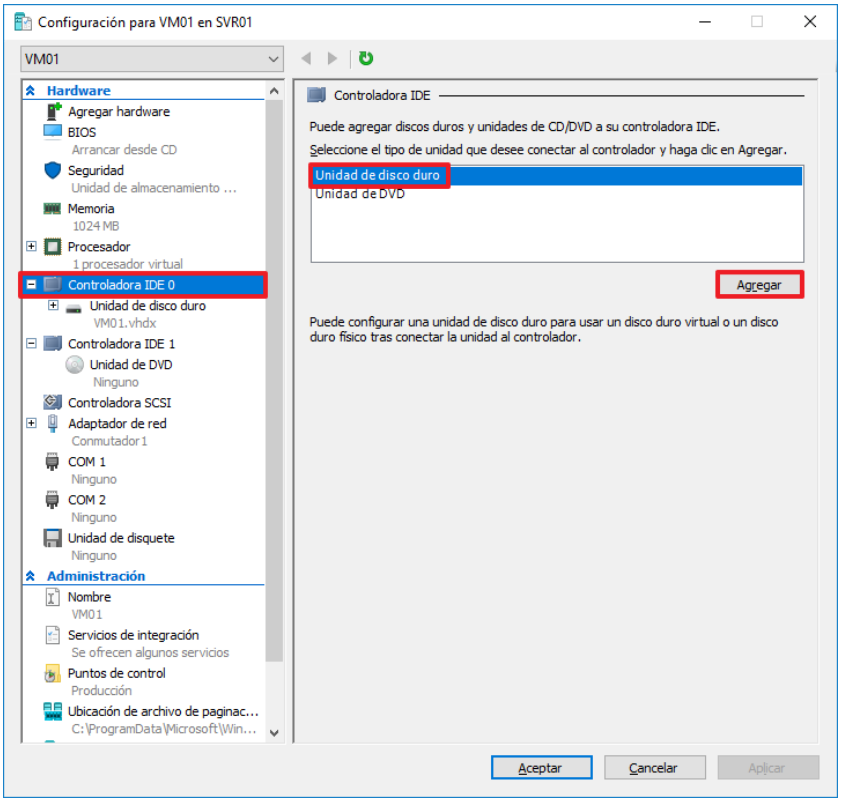
Los discos virtuales son el componente sobre el que se apoyan las máquinas virtuales para almacenar los recursos que se generan al igual que sucede en un equipo real. Este apartado define un ejemplo para crear un disco virtual que pueda ser utilizado con diferentes fines, bien como disco principal de una máquina o como disco adicional.

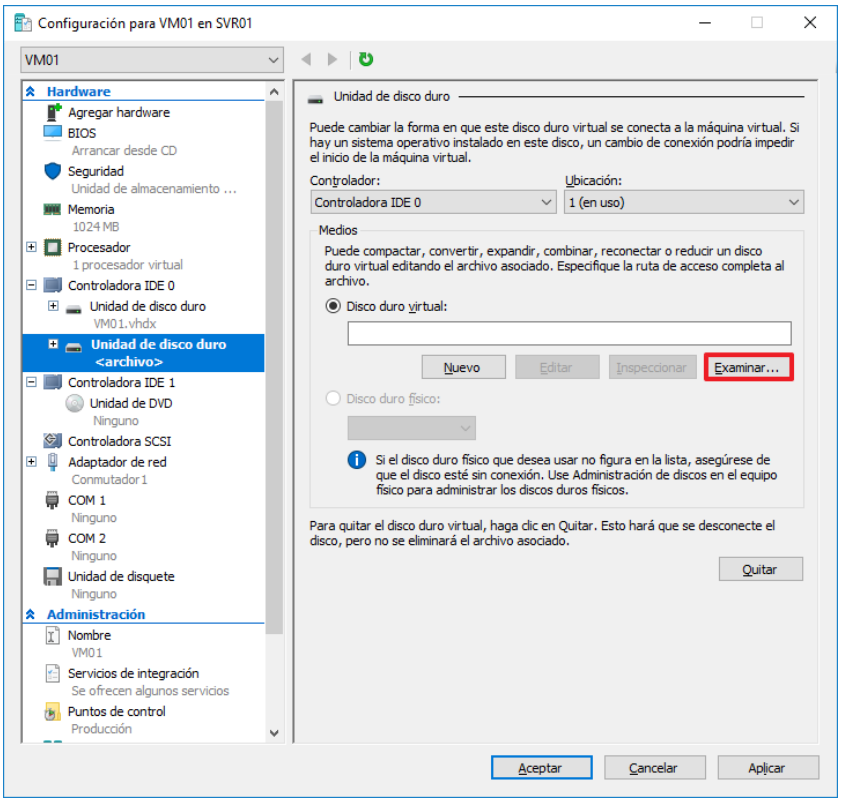
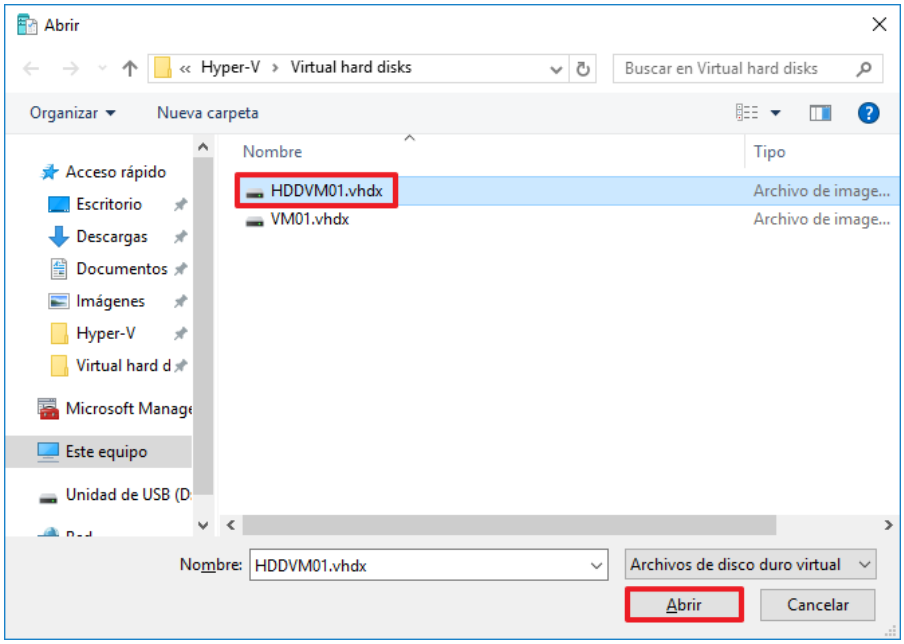
Paso	Descripción
86.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
87.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
88.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 

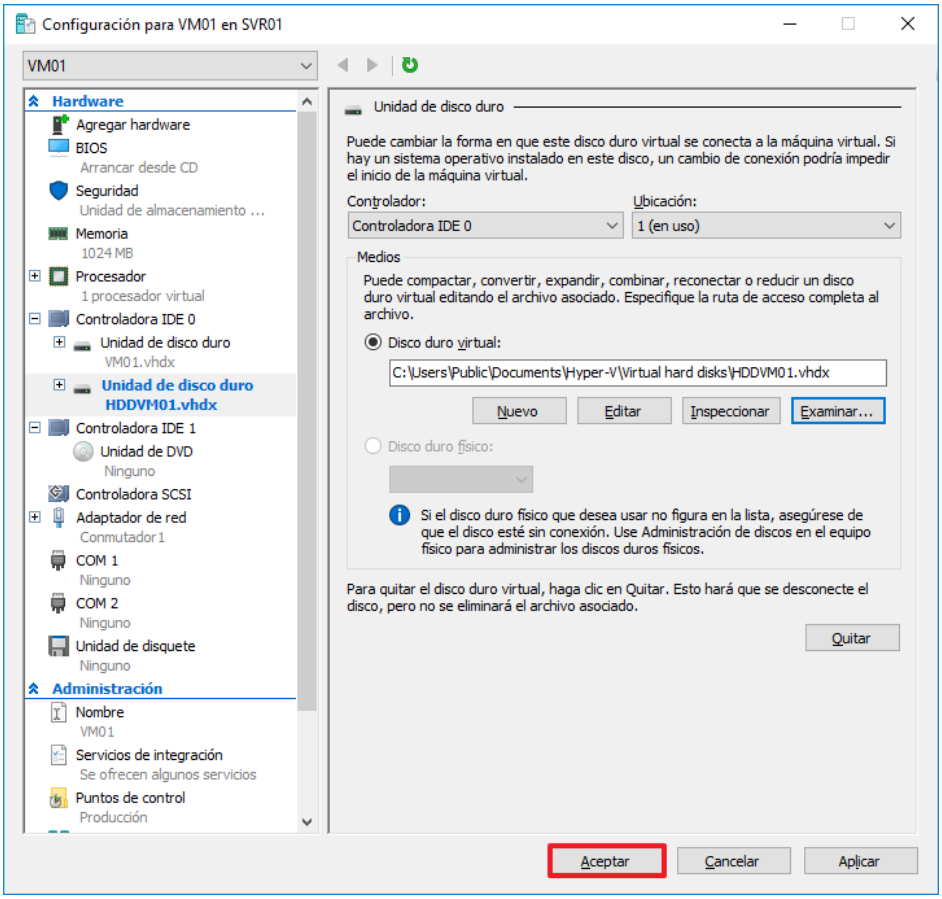
Paso	Descripción
89.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
90.	Dentro de la consola emergente seleccione el servidor de Hyper-V con el botón derecho y seleccione la opción del menú contextual **"Nuevo → Disco duro…".**  **Nota:** En este ejemplo el servidor de denomina "SVR01". Deberá adaptar estos pasos a las configuraciones de su organización.
91.	Aparecerá el asistente para la creación de discos virtuales. En la ventana "Antes de comenzar" pulse "Siguiente >".

Paso	Descripción
92.	En la ventana “Elegir el formato de disco” deberá determinar el formato del disco dependiendo de las necesidades de su organización y de las máquinas virtuales que disponga. Pulse el botón “Siguiente >” para continuar.  **Nota:** En este ejemplo se crea un disco con formato “VHDX”.
93.	En la ventana “Elegir tipo de disco” deberá seleccionar como se dimensiona el disco cuando este almacena datos. Pulse “Siguiente >” cuando haya finalizado.  **Nota:** En este ejemplo se opta por una “Expansión dinámica” del disco.

Paso	Descripción
94.	En la ventana “Especificar el nombre y ubicación” determine el nombre asociado al disco virtual y donde va a ser almacenado. Pulse “Siguiente >” para continuar.  **Nota:** Tenga en consideración que si realizó alguna modificación en el apartado “2.2 CONFIGURACIÓN GENERAL DE HYPER-V” la ubicación por defecto ya deberá estar configurada a la requerida por su organización. En este ejemplo se asigna el nombre “HDDVM01”.
95.	En la ventana “Configurar disco” deberá determinar las necesidades del disco duro creado pudiendo crear un disco en blanco (sin datos) o con datos copiados de otro disco existente. Pulse “Siguiente >” para continuar con el asistente.  **Nota:** En este ejemplo se genera un disco de 100 GB en blanco para asociarlo a una máquina virtual existente.

Paso	Descripción
96.	Por último, en la ventana “Resumen” compruebe que las configuraciones del disco son correctas. En caso afirmativo pulse “Finalizar”. Si por el contrario requiere modificar alguna configuración pulse el botón “< Anterior” hasta llegar a la ventana deseada y modifique la configuración.
97.	Para asignar el disco recién creado seleccione la máquina afectada con el botón derecho y pulse sobre la opción del menú contextual “Configuración…”.  **Nota:** En este ejemplo se hace uso de la máquina virtual “VM01”. Adapte este y los siguientes pasos a las necesidades de su organización. La máquina virtual deberá estar apagada para realizar los siguientes pasos.
98.	Sitúese sobre el apartado “Controladora IDE 0” y en el panel derecho seleccione “Unidad de disco duro”. Pulse sobre “Agregar” para continuar. 

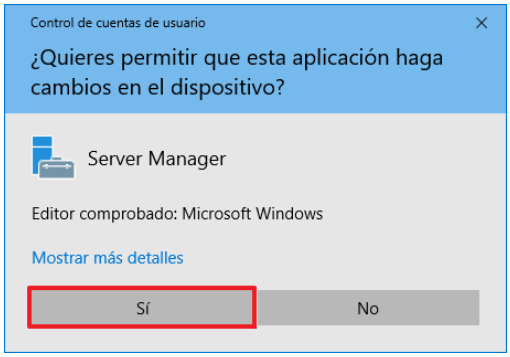
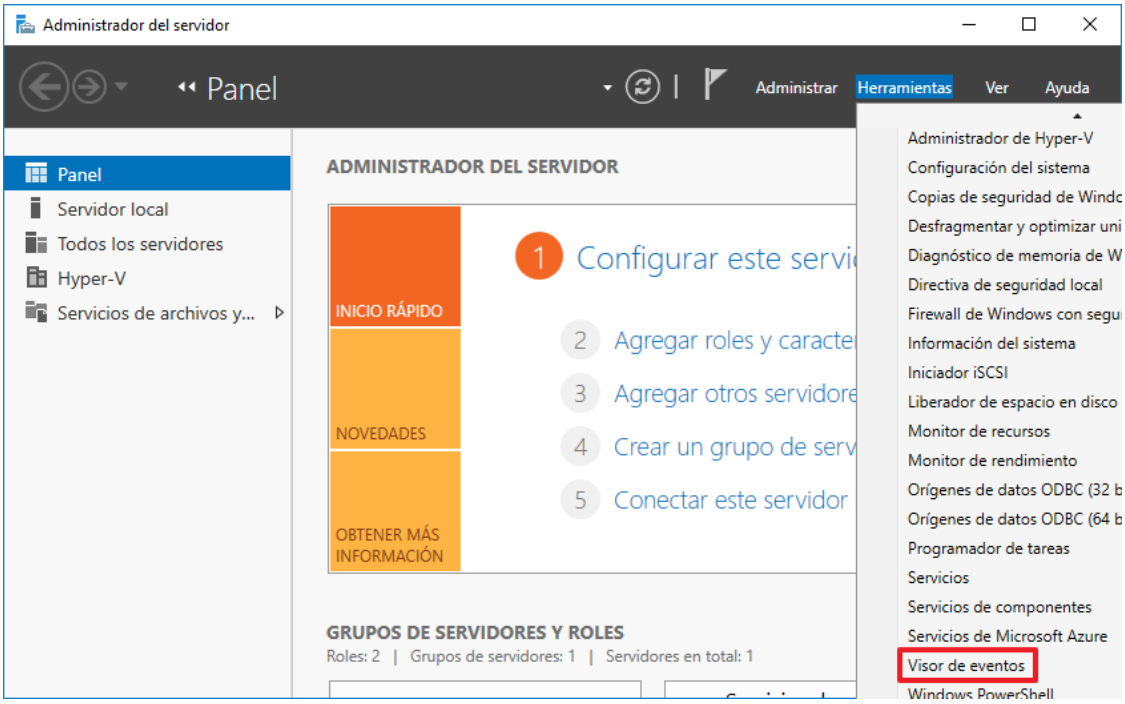
Paso	Descripción
99.	De nuevo en el panel derecho seleccione el botón “Examinar” 
100.	Ubíquese sobre la ruta en la que se creó el disco duro virtual, selecciónelo y pulse el botón “Abrir”. 

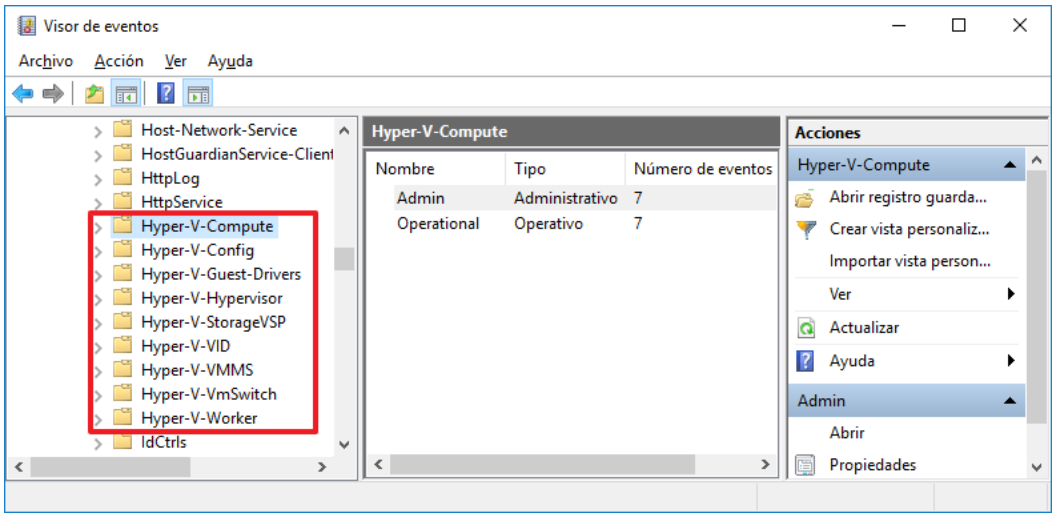
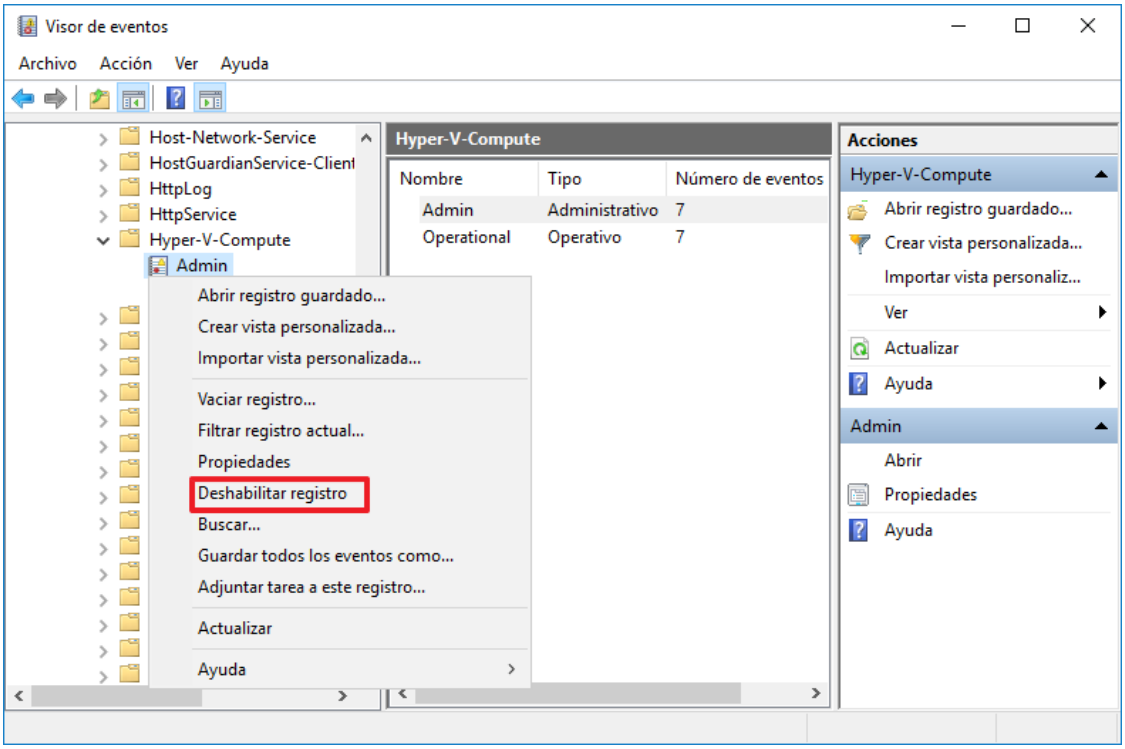
Paso	Descripción
101.	Por último, pulse “Aceptar” para guardar los cambios. A partir de este momento la máquina virtual estará en posesión de un disco duro adicional. 

2.6. REGISTRO DE EVENTOS EN HYPER-V

Todos los eventos que se suceden en el servidor de Hyper-V deben ser recogidos por el equipo con el fin de determinar las acciones realizadas sobre el propio servidor y sobre las máquinas que este alberga.

Paso	Descripción
102.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

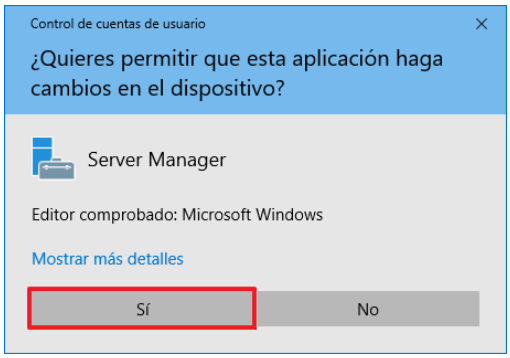
Paso	Descripción
103.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
104.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
105.	Inicie la herramienta "Visor de eventos". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Visor de eventos"**. 

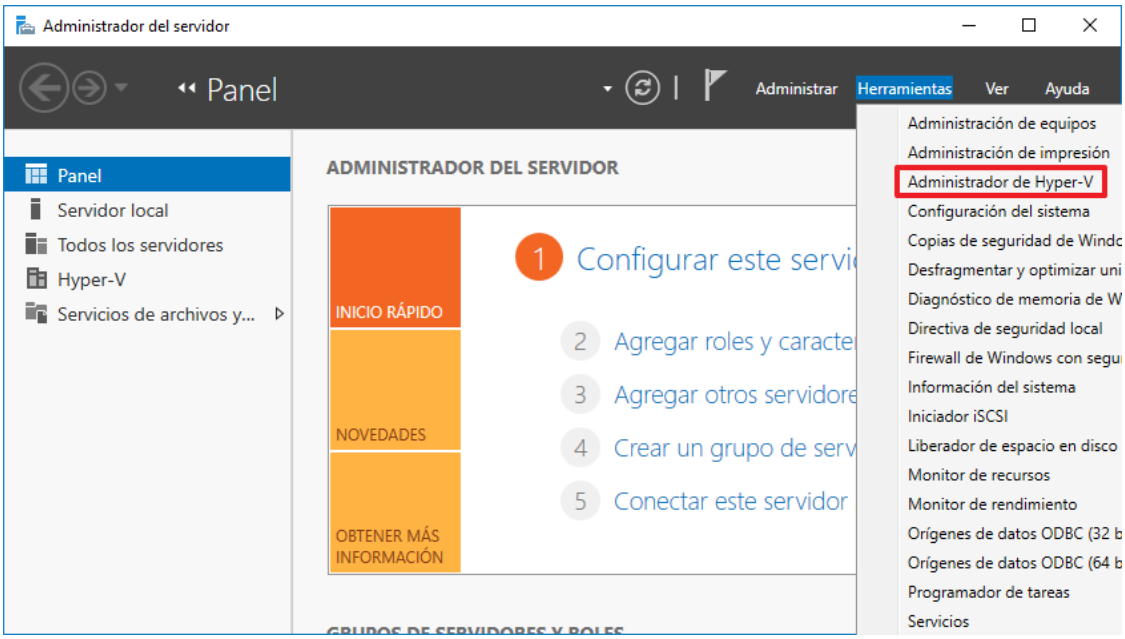
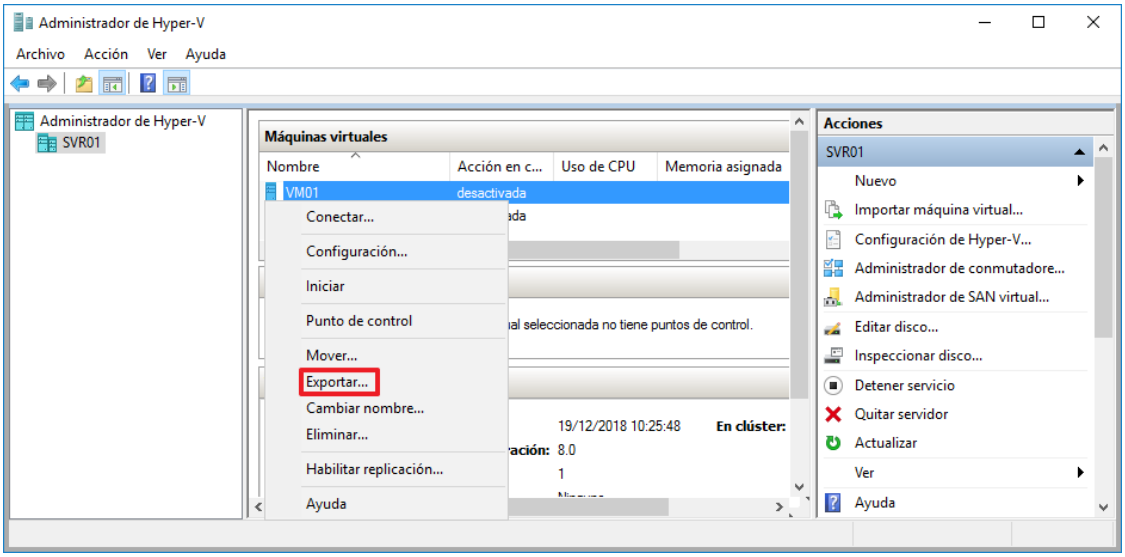
Paso	Descripción
106.	En consola "Visor de eventos" despliegue el nodo **"Visor de eventos (local) → Registro de aplicaciones y servicios → Microsoft → Windows"**. En el listado de carpetas sitúese sobre aquellas que hagan referencia a Hyper-V.  **Nota:** Puede obtener más información acerca de los eventos registrados por Hyper-V en el siguiente enlace: https://blogs.technet.microsoft.com/virtualization/2018/01/23/looking-at-the-hyper-v-event-log-january-2018-edition/
107.	Por último, asegúrese que dentro de cada directorio se encuentra activado el registro haciendo clic derecho sobre cada uno de los elementos. En el caso de que el registro este habilitado aparecerá la opción "Deshabilitar registro". Si por el contrario no se encuentra habilitado el registro aparecerá la opción "Habilitar registro. 

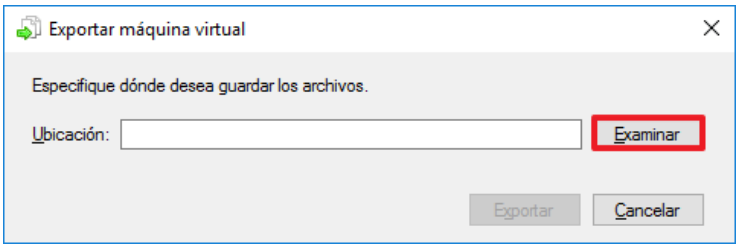
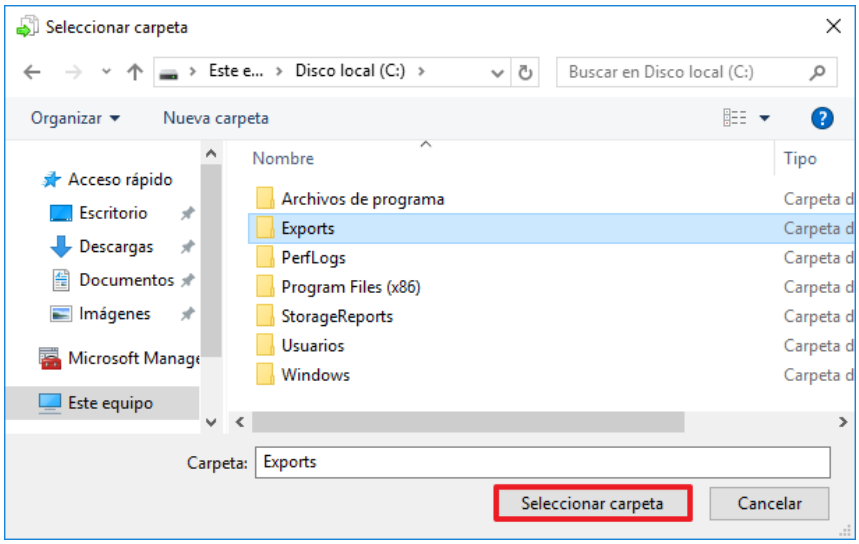
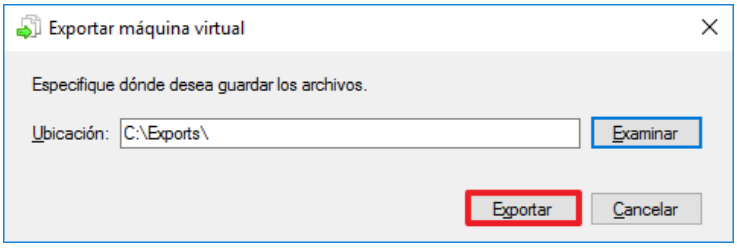
2.7. COPIAS DE SEGURIDAD DE MÁQUINAS VIRTUALES

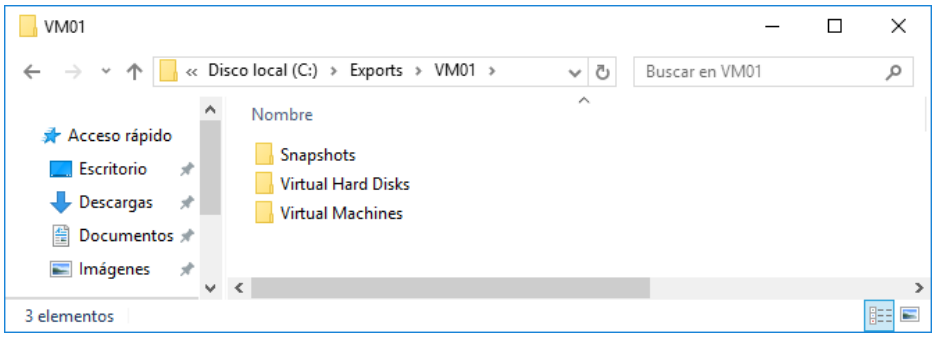
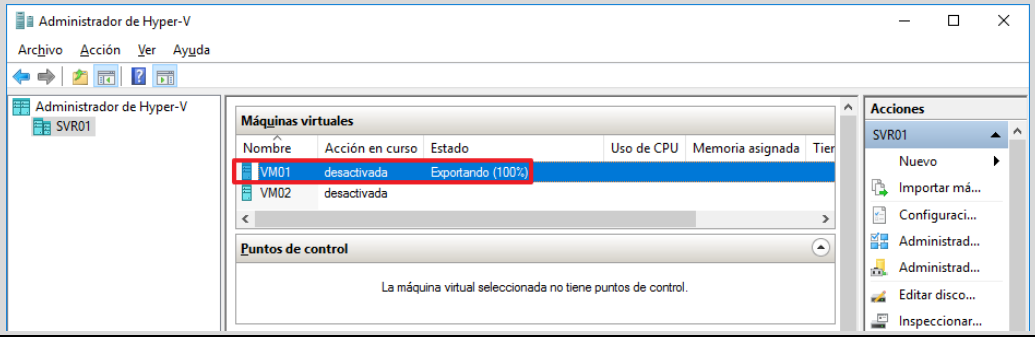
Hyper-V dispone de varias opciones para realizar copias de seguridad de las máquinas con el objetivo de mantener la continuidad y evitar la pérdida de datos. Aunque tal y como se explicó en apartados anteriores es posible configurar un servidor como equipo de réplicas se va a optar por una opción que permite realizar copias si no se dispone de un servidor adicional.

2.7.1. EXPORTAR MÁQUINAS VIRTUALES

Paso	Descripción
108.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
109.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
110.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 

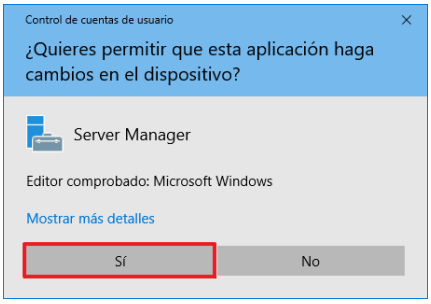
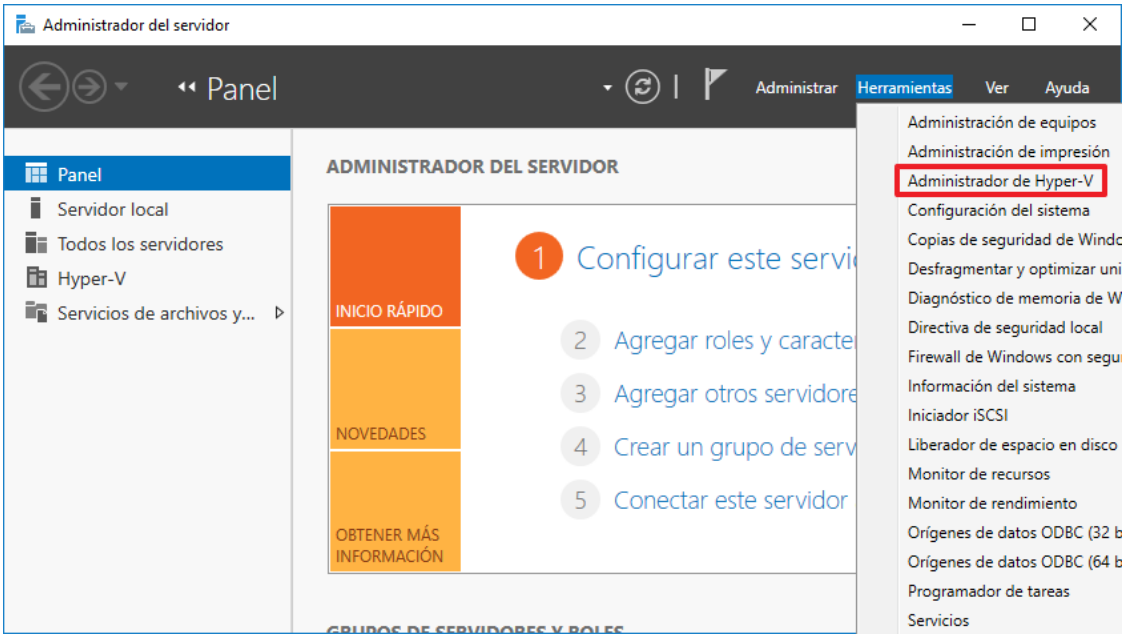
Paso	Descripción
111.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
112.	Seleccione la máquina virtual sobre la que desea realizar una copia de seguridad y pulse sobre la opción "Exportar…".  **Nota:** En este ejemplo se realiza la exportación de la máquina "VM01".

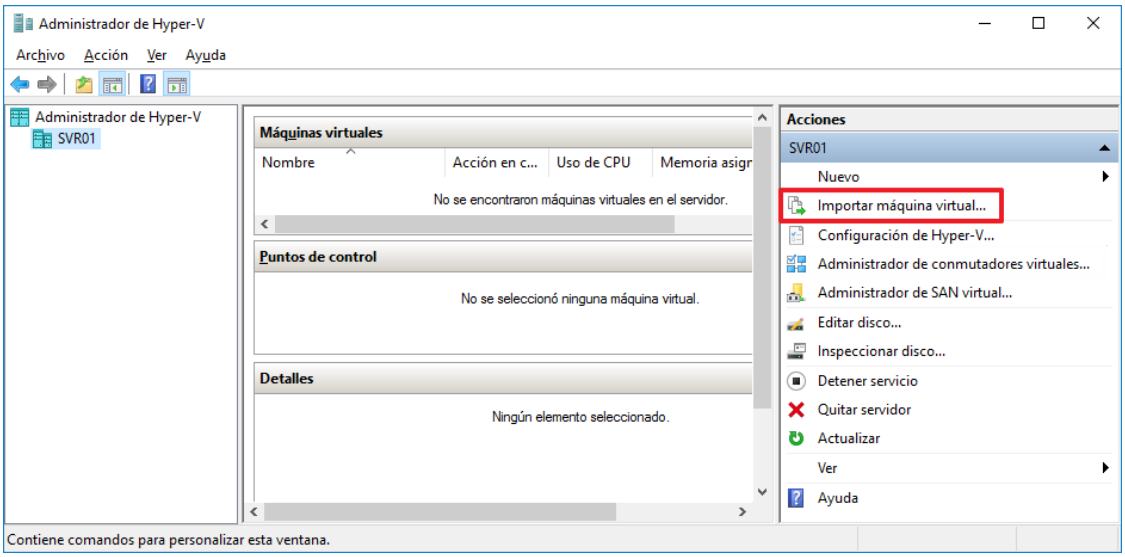
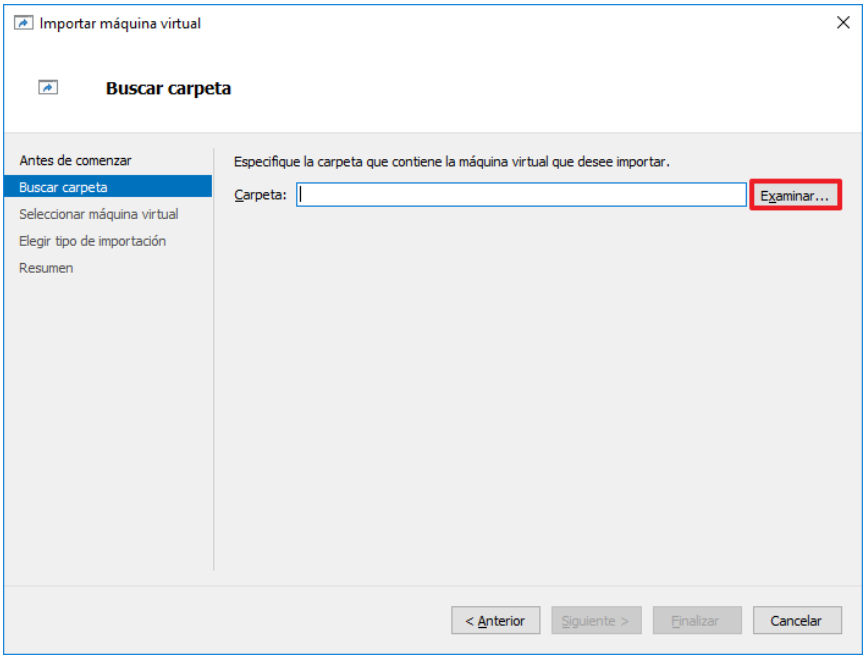
Paso	Descripción
113.	En la ventana emergente pulse sobre el botón “Examinar”. 
114.	Seleccione la ubicación sobre la que desea exportar la máquina y pulse sobre el botón “Seleccionar carpeta”.  **Nota:** En este ejemplo se utiliza el directorio “Exports” ubicado en “C:\”.
115.	Pulse sobre el botón “Exportar” para comenzar con la copia. 

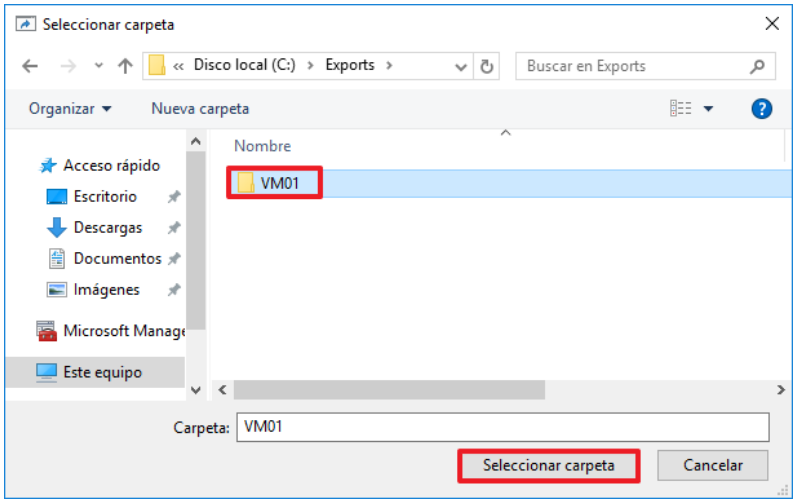
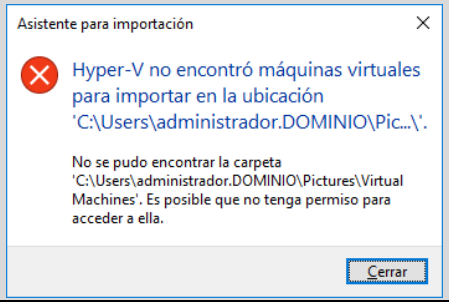
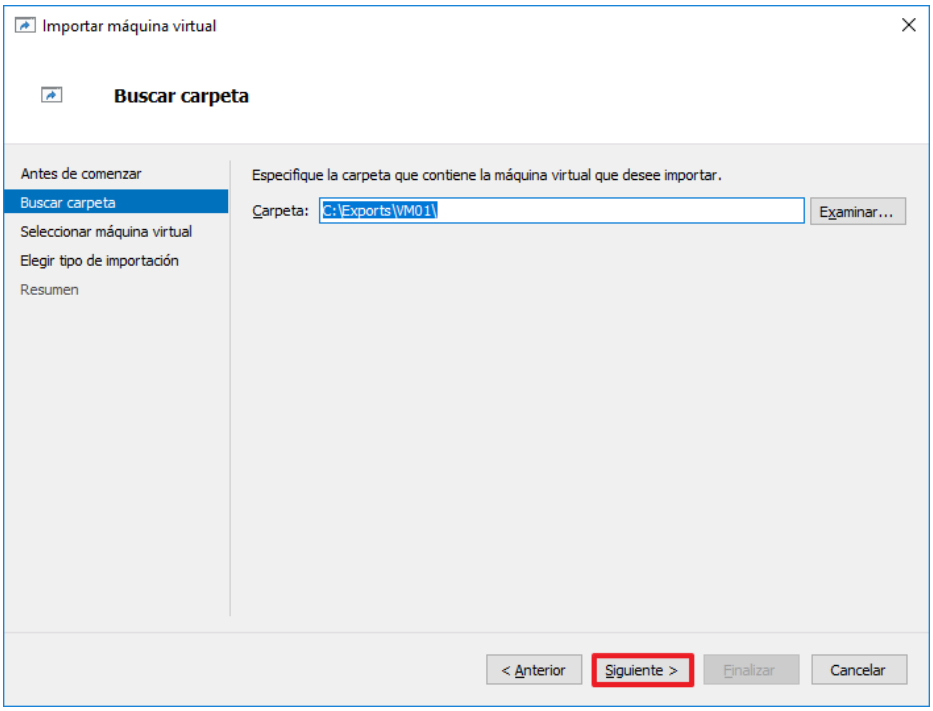
Paso	Descripción
116.	Cuando el proceso haya finalizado la consola de Hyper-V lo notificará en el apartado correspondiente al "Estado" y dentro del directorio seleccionado se habrá generado un directorio con todos los componentes de la máquina virtual.  **Nota:** Dependiendo del tamaño de la máquina el tiempo podrá variar. La consola de Hyper-V mostrará en todo caso el porcentaje de estado. 

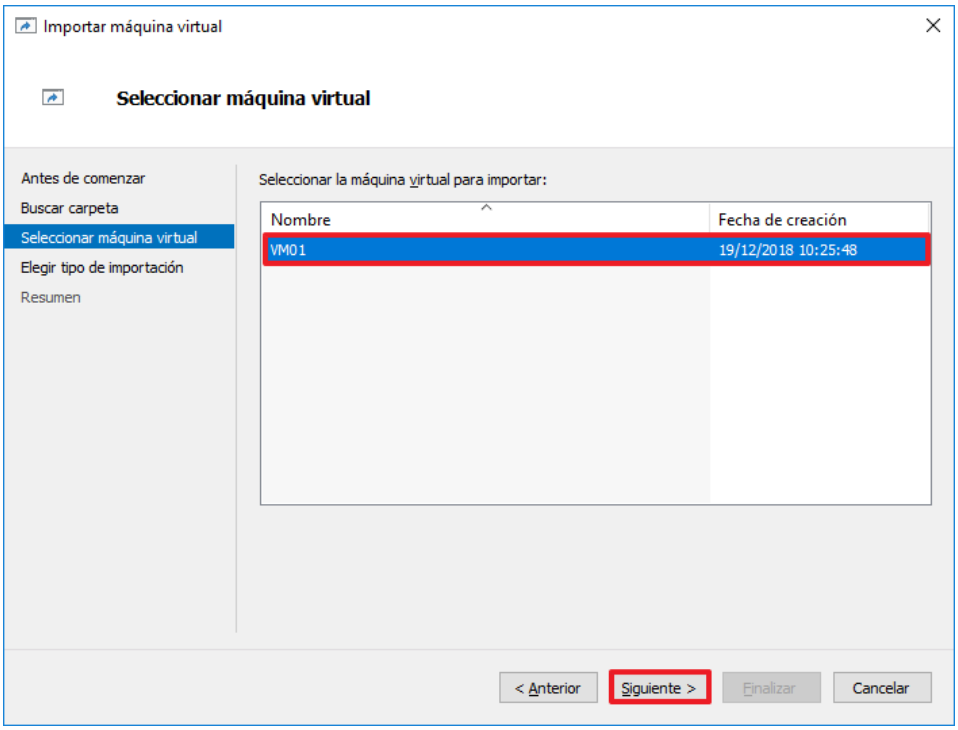
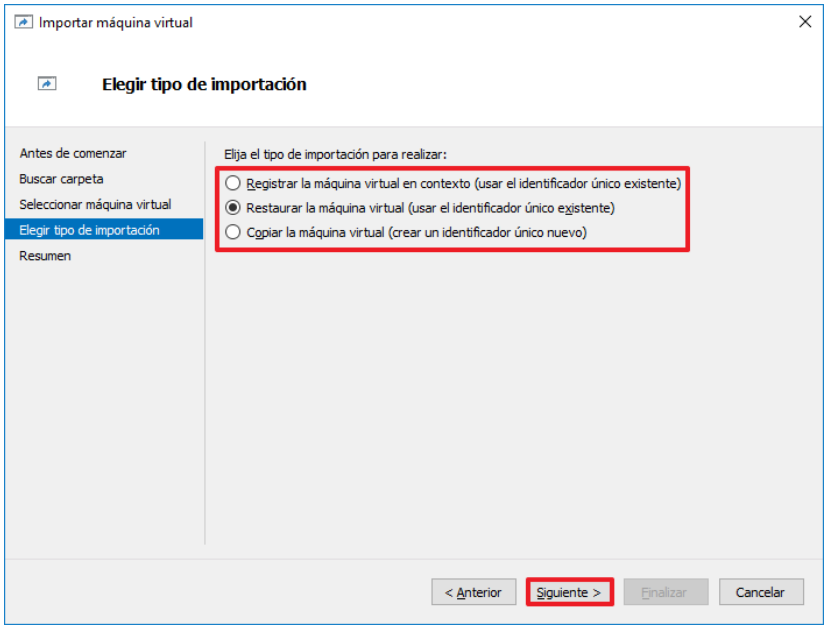
2.7.2. IMPORTAR MÁQUINAS VIRTUALES

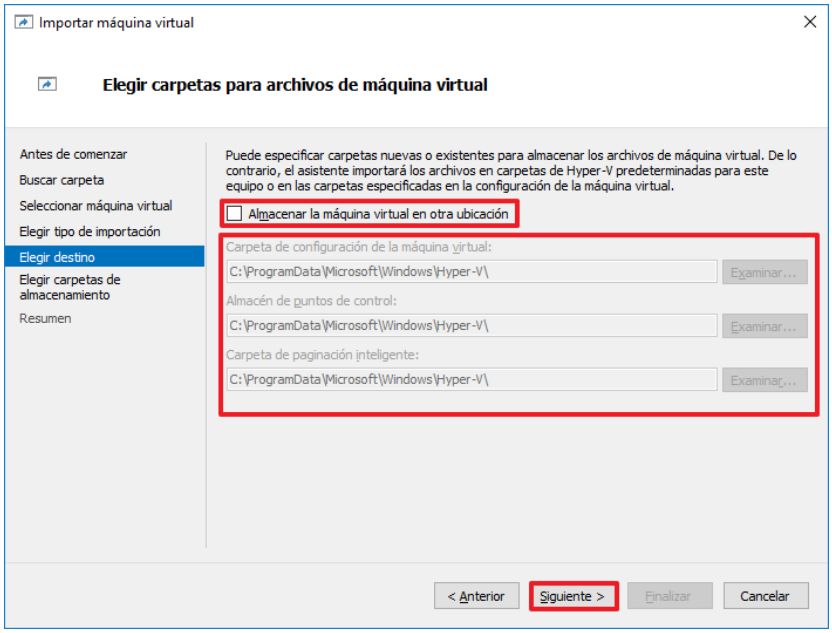
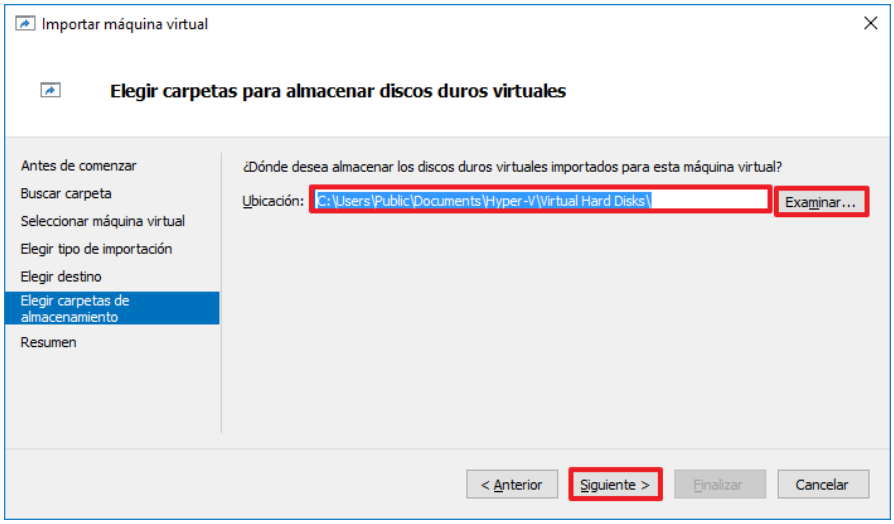
Paso	Descripción
117.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

Paso	Descripción
118.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
119.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
120.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 

Paso	Descripción
121.	Seleccione la opción del panel derecho “Importar máquina virtual…” 
122.	Se iniciará el asistente para importar una máquina virtual. Pulse “Siguiente >” en la ventana “Antes de comenzar”.
123.	En la ventana “Buscar carpeta” pulse sobre el botón “Examinar…”. 

Paso	Descripción
124.	A continuación, seleccione el directorio donde se encuentre la máquina virtual y pulse sobre "Seleccionar carpeta".  **Nota:** Si selecciona una ubicación incorrecta el asistente notificará un error. 
125.	Pulse el botón "Siguiente >" para continuar con la importación. 

Paso	Descripción
126.	Seleccione la máquina virtual que desea importar y pulse “Siguiente >”  **Nota:** Es posible que la ruta indicada posea varias máquinas virtuales para importar, por lo que deberá seleccionar aquella que corresponda.
127.	En la ventana elegir tipo de importación seleccione la opción más adecuado dependiendo de la operación a realizar con la máquina. Pulse “Siguiente >” para finalizar con la importación”  **Nota:** En este ejemplo se hace uso de la opción “Restaurar la máquina virtual”. Dependiendo de la opción seleccionada deberá ejecutar más o menos pasos en el asistente.

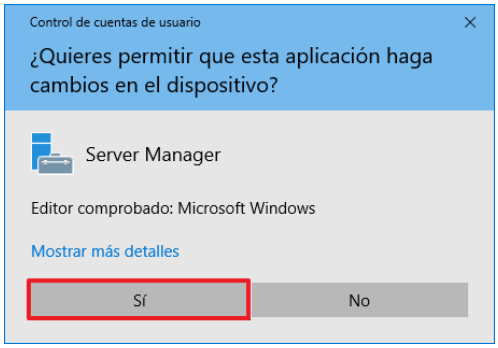
Paso	Descripción
128.	En la ventana “Elegir destino” deberá establecer si lo desea una ruta para cada una de las configuraciones de la máquina virtual. Pulse “Siguiente >” cuando haya finalizado.  **Nota:** En este ejemplo se opta por ubicar los archivos en las rutas por defecto definidas en apartados anteriores.
129.	Al igual que sucedía en el paso anterior deberá ahora establecer la ubicación para los discos de la máquina virtual. Si no indica dicha ubicación se almacenarán en la ubicación predefinida en apartados anteriores. Pulse “Siguiente >” para continuar. 
130.	Por último, en la ventana “Resumen” compruebe que las configuraciones de la máquina virtual son correctas. En caso afirmativo pulse “Finalizar”. Si por el contrario requiere modificar alguna configuración pulse el botón “< Anterior” hasta llegar a la ventana deseada y modifique la configuración.

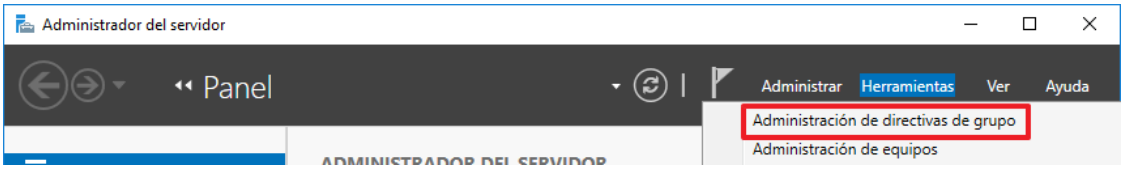
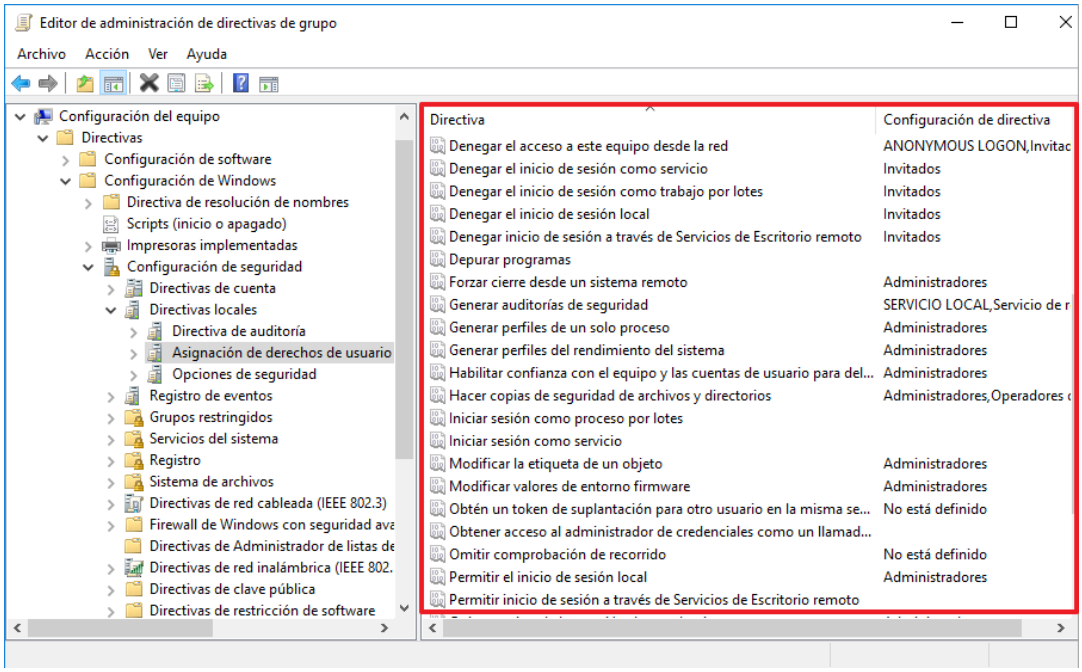
2.8. DERECHOS DE ACCESO SOBRE SISTEMAS OPERATIVOS MS WINDOWS VIRTUALIZADOS

Los permisos de acceso sobre las máquinas virtuales que contiene el servicio de Hyper-V debe quedar limitado a los usuarios legítimos a ello por lo tanto será necesario establecer los permisos necesarios para limitar dicha conectividad.

Deberá tener en consideración la asignación de permisos diferenciando si la conexión se realiza a un servidor o un equipo cliente. Deberá por tanto generar un objeto GPO incremental o modificar la configuración establecida con el fin de permitir o denegar el inicio de sesión sobre las máquinas virtuales.

En el presente apartado se trata el ejemplo de configurar dicha asignación de permisos a través del objeto GPO que configura Hyper-V.

Paso	Descripción
131.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
132.	Ejecute el “Administrador del Servidor” desde el icono correspondiente. 
133.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 

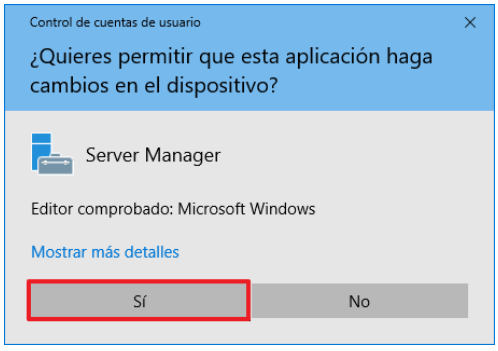
Paso	Descripción
134.	A continuación, inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor”, abierta en pasos anteriores, seleccione **“Herramientas → Administración de directivas de grupo”.** 
135.	Los objetos de políticas de grupo para Controladores de Dominio y Servidores miembros especifican unos derechos de usuario siguiendo planteamientos de seguridad que aplican los principios de mínimo privilegio y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les hayan asignado derechos determinados para la administración o gestión de los sistemas. Si esto fuera así, deberá realizar las modificaciones pertinentes sobre el objeto de política de grupo que aplique sobre el sistema operativo virtualizado o bien editando la configuración de política de grupo local en el caso de un equipo no perteneciente a un dominio.
136.	Sobre el objeto de GPO que se quiere modificar, deberá pulsar clic derecho y seleccionar “Editar” en el menú desplegado.
137.	Una vez abierto el “Editor de administración de directivas de grupo”, despliegue la política y sitúese en la siguiente ruta: **“Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”** 
138.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales de conexión.
139.	Guarde la configuración cerrando la ventana de editor de administración de directivas de grupo.

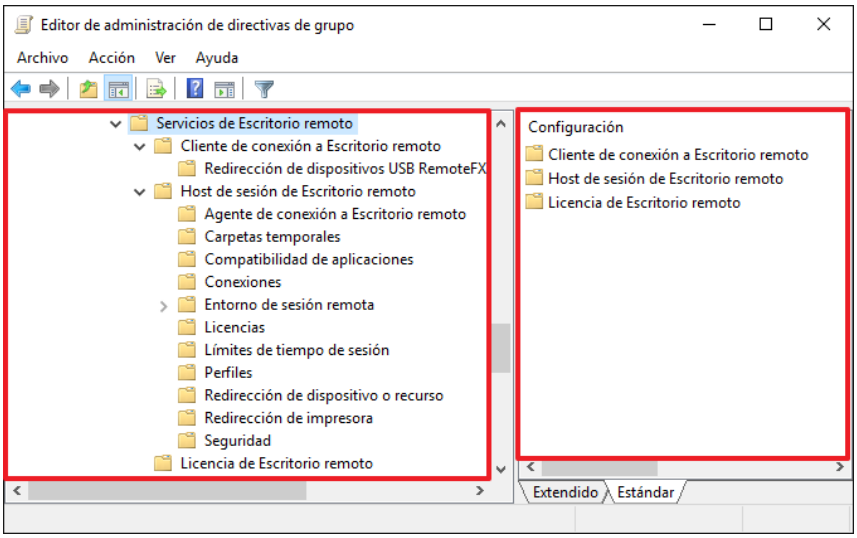
2.9. ACCESO REMOTO SOBRE SISTEMAS OPERATIVOS MS WINDOWS VIRTUALIZADOS

Del mismo modo que en el punto anterior no basta con conceder permisos sobre los equipos cliente o servidores ubicados dentro del servidor de Hyper-V sino que además será necesario establecer los mecanismos seguros para las conexiones remotas a las máquinas virtuales que almacena Hyper-V.

En el presente apartado se definen las medidas a tomar en el caso de realizar una conexión remota a través del servicio Escritorio Remoto de Windows. Para definir dicha configuración deberá hacer uso de un objeto GPO incremental que configure la seguridad de dicho servicio o editar la configuración de un objeto GPO ya aplicado.

Para el presente ejemplo se realiza un ejemplo de configuración para escritorio remoto que asegure la conexión de este servicio al servidor de Hyper-V.

Paso	Descripción
140.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
141.	Ejecute el “Administrador del Servidor” desde el icono correspondiente. 
142.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 

Paso	Descripción
143.	A continuación, inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor”, abierta en pasos anteriores, seleccione **“Herramientas → Administración de directivas de grupo”.** 
144.	Los elementos de plantillas administrativas permiten establecer la configuración segura a realizar sobre una conexión basada en servicios de escritorio remoto. Esta configuración permite que las conexiones realizadas a servidores y equipos cliente asegure la integridad de la conexión. Para establecer dicha configuración, deberá realizar las modificaciones pertinentes sobre el objeto de política de grupo que aplique sobre el sistema operativo virtualizado o bien editando la configuración de política de grupo local en el caso de un equipo no perteneciente a un dominio.
145.	Sobre el objeto de GPO que se quiere modificar, deberá pulsar clic derecho y seleccionar “Editar” en el menú desplegado.
146.	Una vez abierto el “Editor de administración de directivas de grupo”, despliegue la política y sitúese en la siguiente ruta: **“Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Servicios de Escritorio remoto”** 
147.	Modifique las directivas, estableciendo una configuración segura para el acceso remoto tanto a servidores como equipos cliente.
148.	Guarde la configuración cerrando la ventana de editor de administración de directivas de grupo.
149.	Adicionalmente a esta configuración deberá establecer los parámetros de red que permitan realizar la comunicación en red. Para ello haga uso de nuevo del objeto GPO correspondiente y configurando el firewall para que permita la conexión entre equipos.

ANEXO A.2.2. LISTA DE COMPROBACIÓN DE HYPER-V SOBRE WINDOWS SERVER 2016 PARA SERVIDORES QUE LES SON DE APLICACIÓN LA CATEGORÍA BASICA DEL ENS

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía "ANEXO A.2.1 PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE HYPER-V SOBRE SERVIDORES WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS".

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

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

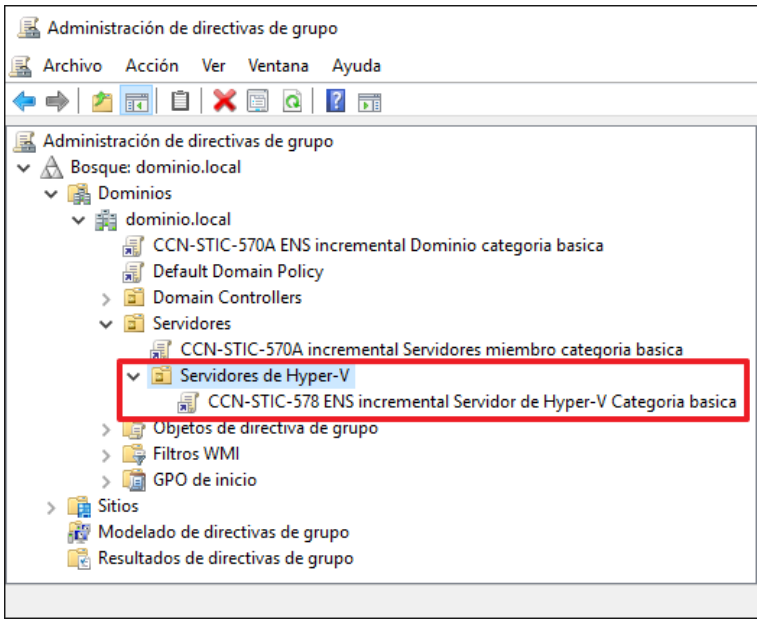
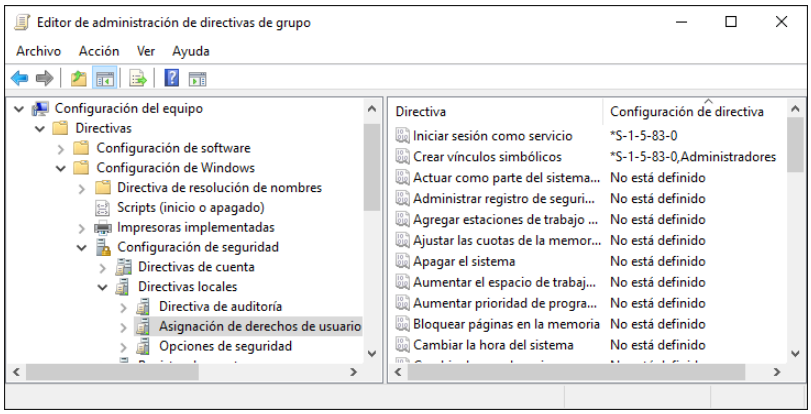
Posteriormente, se deberán realizar las comprobaciones en el propio servidor de Hyper-V, para lo que será necesario ejecutar diferentes consolas de administración y herramientas del sistema, las cuales estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario con privilegios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

a) En el Controlador de Dominio:
   i. Usuarios y equipos de Active Directory (dsa.msc).
   ii. Administrador de directivas de grupo (gpmc.msc).
   iii. Editor de objetos de directiva de grupo (gpedit.msc).

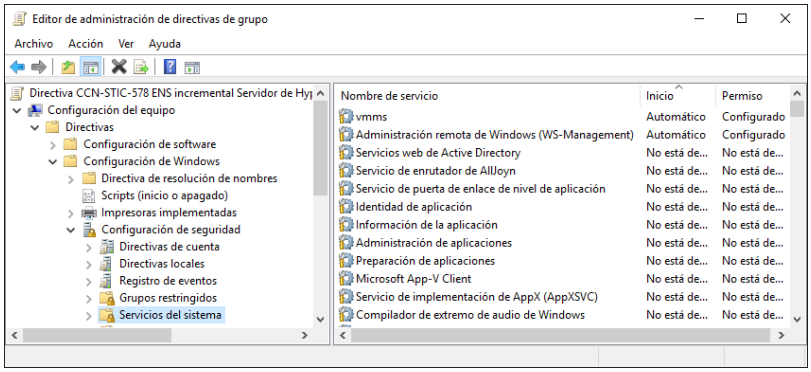
b) En el servidor de Hyper-V:
   i. Administrador de Windows (explorer.exe).
   ii. PowerShell (powershell.exe).
   iii. Servicios (services.msc).
   iv. Editor de objetos de directiva de grupo (gpedit.msc).
   v. Administrador de Hyper-V (virtmgmt.msc).
   vi. Visor de eventos (eventvwr.msc).

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

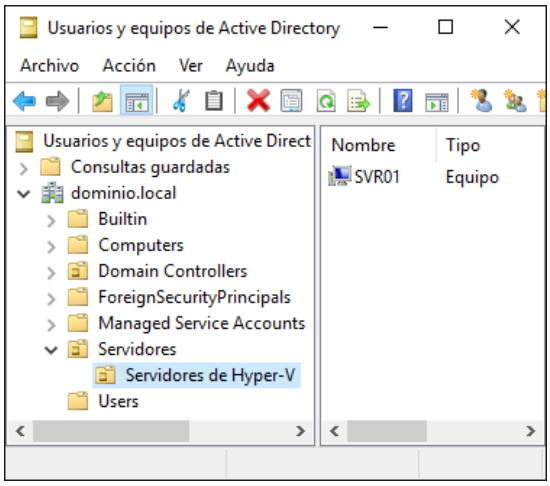
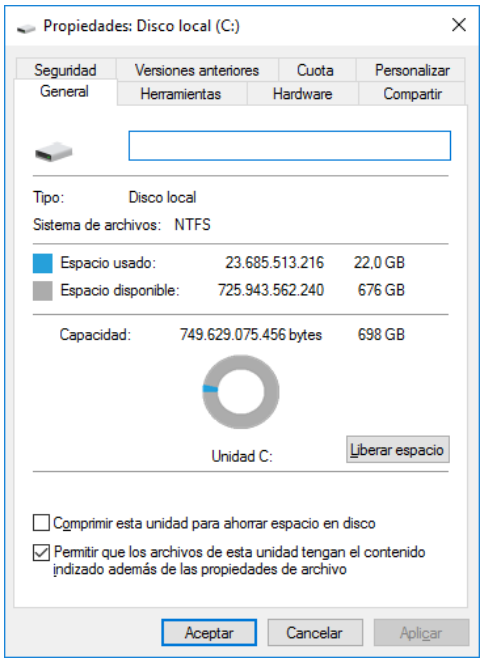
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un Controlador de Dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>2. Verifique que está creada la directiva “CCN-STIC-578 ENS incremental Servidor de Hyper-V Categoria basica”.</td><td></td><td>Utilice el Administrador de directivas de grupo (Inicio → Herramientas administrativas → Administración de directivas de grupo) y despliegue el menú en árbol hasta llegar a la unidad organizativa “Servidores de Hyper-V” que se encuentra en la Unidad Organizativa “Servidores”. Verifique que está creada la política “CCN-STIC-578 ENS incremental Servidor de Hyper-V Categoria basica”.
 
</td></tr>
<tr><td>3. Verifique los valores de la asignación de derechos de usuario.</td><td></td><td>Utilizando el editor de objetos de directiva de grupo, verifique que la directiva “CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria basica” tiene los siguientes valores de asignación de derechos de usuario en el siguiente nodo:
Directiva CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Iniciar sesión como servicio</td><td>Máquinas virtuales (*S-1-5-83-0)</td><td></td></tr>
<tr><td>Crear vínculos simbólicos</td><td>Máquinas virtuales (*S-1-5-83-0)
Administradores</td><td></td></tr>
</table></td></tr>
</table>

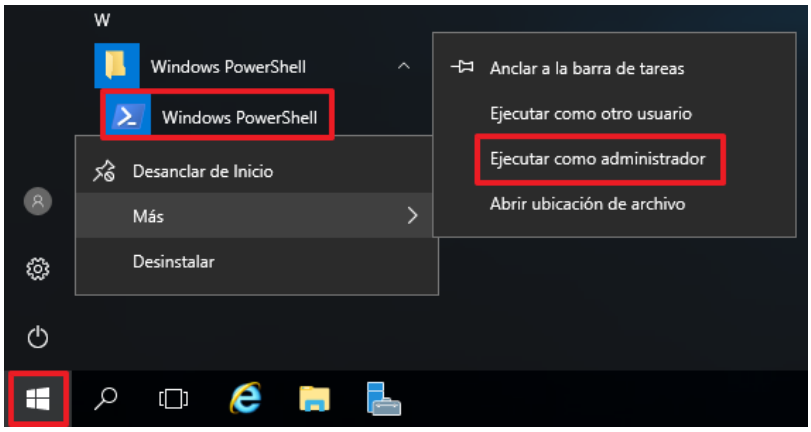
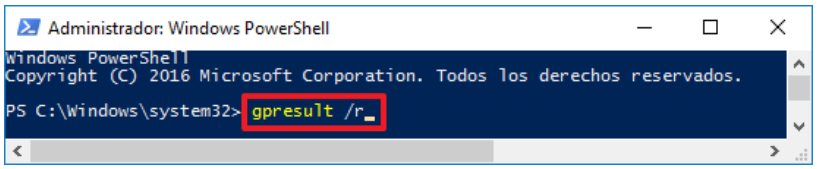
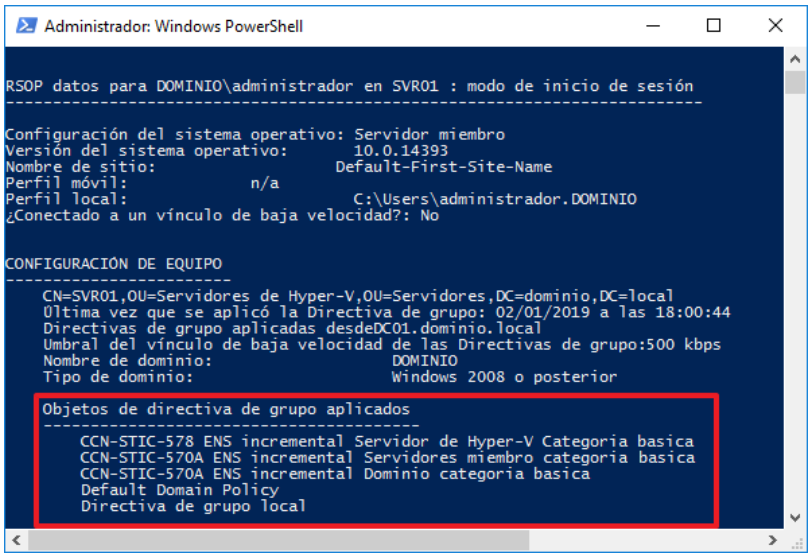
Comprobación	OK/NOK	Cómo hacerlo
4. Verifique los valores de servicios.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria basica" tiene los siguientes valores de asignación de derechos de usuario en el siguiente nodo: **Directiva CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del Sistema.** 

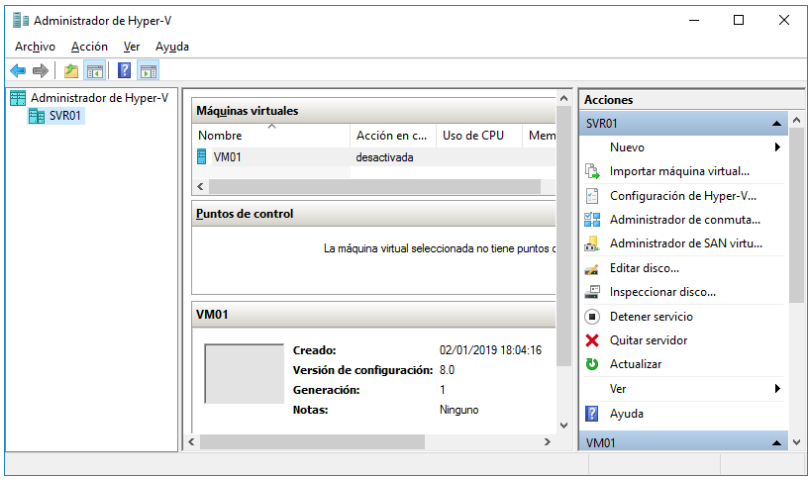
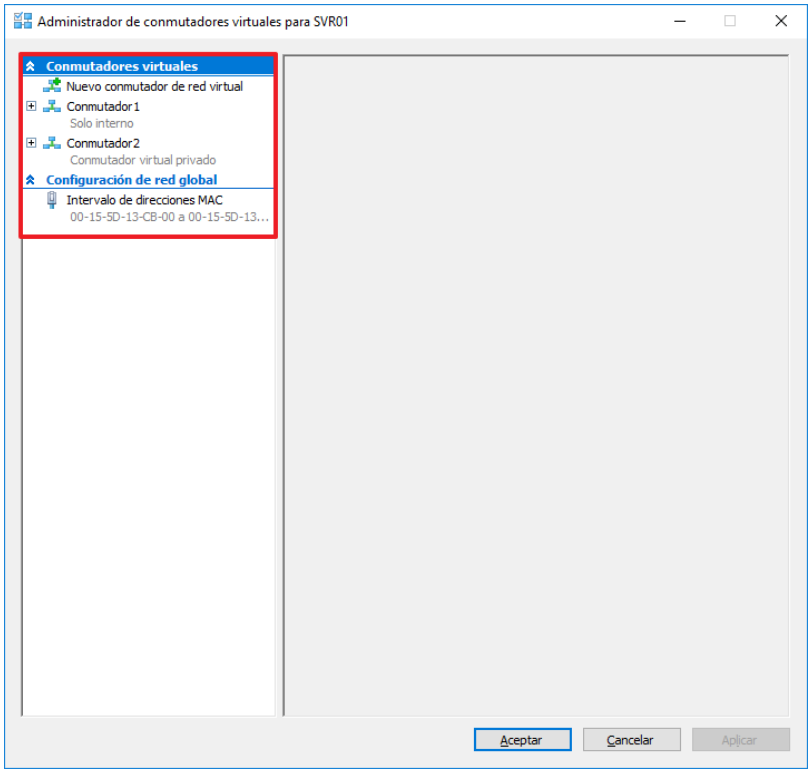
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Administración de máquinas virtuales de Hyper-V	vmms	Automático	Configurado	
Agente de host NC	nchostagent	Deshabilitado	Configurado	
Aislamiento de claves CNG	keyiso	Automático	Configurado	
Instantáneas de volumen	vss	Manual	Configurado	
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado	
Servicio de cierre de invitado de Hyper-V	vmicshutdown	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado	
Servicio de proceso de host de Hyper-V	vmcompute	Manual	Configurado	
Servicio de proxy DNS	DNSProxy	Deshabilitado	Configurado	
Servicio de red de host	hns	Manual	Configurado	
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado	
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual	Configurado	
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado	
Software Load Balancer Host Agent	SlbHostAgent	Manual	Configurado	

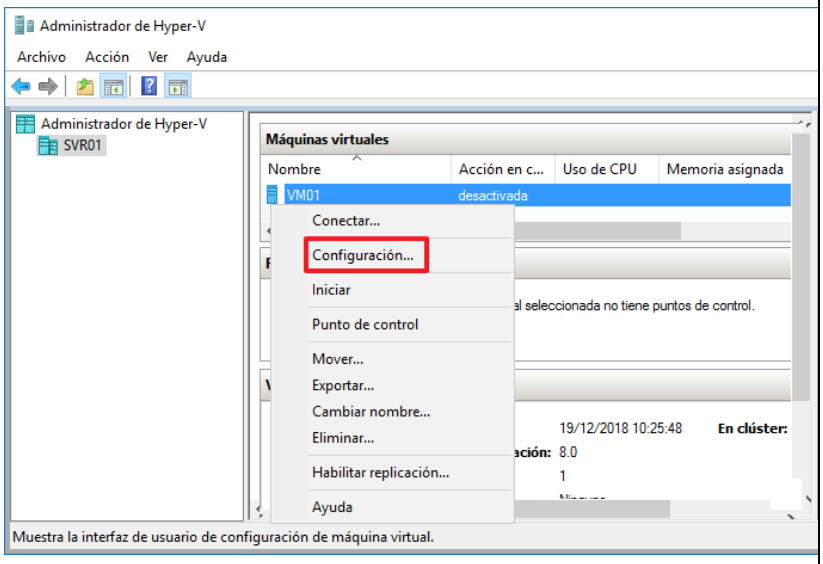
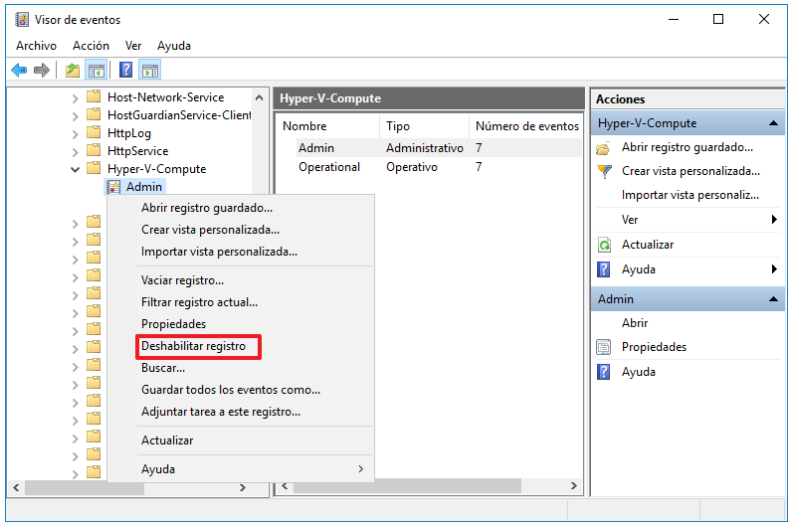
Comprobación	OK/NOK	Cómo hacerlo
5. Verifique que los servidores de Hyper-V están dentro de las Unidades Organizativas adecuada		Utilice la herramienta Usuarios y equipos de Active Directory (**Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**) y seleccione las unidades organizativas que contienen los Servidores de Hyper-V. Compruebe que existe un objeto de tipo equipo por cada uno de los servidores de Hyper-V que se están asegurando.  **Nota:** Para el desarrollo de esta guía se utiliza la Unidad Organizativa "Servidores de Hyper-V".
6. Inicie sesión en un Servidor de Hyper-V		Para completar el resto de la lista de verificación deberá iniciar sesión con una cuenta que tenga permisos de administrador del dominio.
7. Verifique el sistema de ficheros de los volúmenes		Utilizando el explorador de Windows (botón derecho sobre **Inicio → Explorador de archivos**, botón derecho sobre la unidad C:\), verifique en las propiedades de cada partición el uso del sistema de archivos NTFS o cualquier sistema de archivos que permita la aplicación de ACL's. 

Comprobación	OK/NOK	Cómo hacerlo
8. Verifique que están instalados los componentes que se indican		En el "Administrador del Servidor", pulse sobre la opción "Servidor Local" situado en el lateral izquierdo y diríjase a la parte final de la ventana principal, "Roles y características", por medio del scroll lateral derecho. Compruebe que se encuentran instalados los siguientes componentes.
	Rol	**OK/NOK**
	Hyper-V	
9. Verifique los valores de servicios.		Ejecute el complemento "Servicios" (ejecutando "services.msc" desde **"Inicio → Ejecutar…"**) y compruebe el tipo de inicio de los servicios que se indican a continuación.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Administración de máquinas virtuales de Hyper-V	vmms	Automático	Configurado	
Agente de host NC	nchostagent	Deshabilitado	Configurado	
Aislamiento de claves CNG	keyiso	Automático	Configurado	
Instantáneas de volumen	vss	Manual	Configurado	
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado	
Servicio de cierre de invitado de Hyper-V	vmicshutdown	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado	
Servicio de proceso de host de Hyper-V	vmcompute	Manual	Configurado	
Servicio de proxy DNS	DNSProxy	Deshabilitado	Configurado	
Servicio de red de host	hns	Manual	Configurado	
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado	
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual	Configurado	
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado	
Software Load Balancer Host Agent	SlbHostAgent	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo
10. Inicie la consola de PowerShell		Ejecute la consola de PowerShell. Para ello pulse sobre "Inicio", seleccione **"Windows Powershell → Windows Powershell"** con el botón derecho y pulse sobre la opción **"Más → Ejecutar como administrador"**. 
11. Verifique que se están aplicando los objetos GPO necesarios		Verifique que se están aplicando las GPOs correspondientes ejecutando el comando "gpresult /r". 
12. Verifique que se están aplicando los objetos GPO necesarios		Verifique que se aplican los siguientes objetos GPO y en el siguiente orden. – CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria basica. – CCN-STIC-570A ENS incremental Servidores miembro categoria basica. – CCN-STIC-570A ENS incremental Dominio categoria basica. 

Comprobación	OK/NOK	Cómo hacerlo
13. Verifique que la instalación se ha realizado correctamente		Utilizando la herramienta de administración de Hyper-V (ejecutando "virtmgmt.msc" desde **"Inicio → Ejecutar…"**), verifique que la consola se inicia y presenta el servidor local como un servidor de Hyper-V. 
14. Verifique que se disponen de conmutadores de red virtuales configurados		Utilizando la herramienta de administración de Hyper-V (ejecutando "virtmgmt.msc" desde **"Inicio → Ejecutar…"**), verifique haciendo uso de la opción "Administrador de conmutadores virtuales" del panel de acciones, que existen conmutadores virtuales configurados. 

Comprobación	OK/NOK	Cómo hacerlo
15. Verifique que existen máquinas y que su configuración es adecuada		Utilizando la herramienta de administración de Hyper-V (ejecutando "virtmgmt.msc" desde **"Inicio → Ejecutar…"**), verifique que existen máquinas virtuales y que estas poseen la configuración adecuada haciendo clic derecho sobre cada una de ellas y seleccionando la opción del menú contextual "Configuración". 
16. Verifique que la auditoría sobre el servidor de Hyper-V se encuentra activada		Utilizando la herramienta de visor de eventos de Windows (ejecutando "eventvwr.msc" desde **"Inicio → Ejecutar…"**), verifique que la auditoría del servidor de Hyper-V se encuentra activada en todos sus componentes haciendo clic derecho sobre cada uno de sus registros. 

ANEXO A.3. CATEGORÍA MEDIA

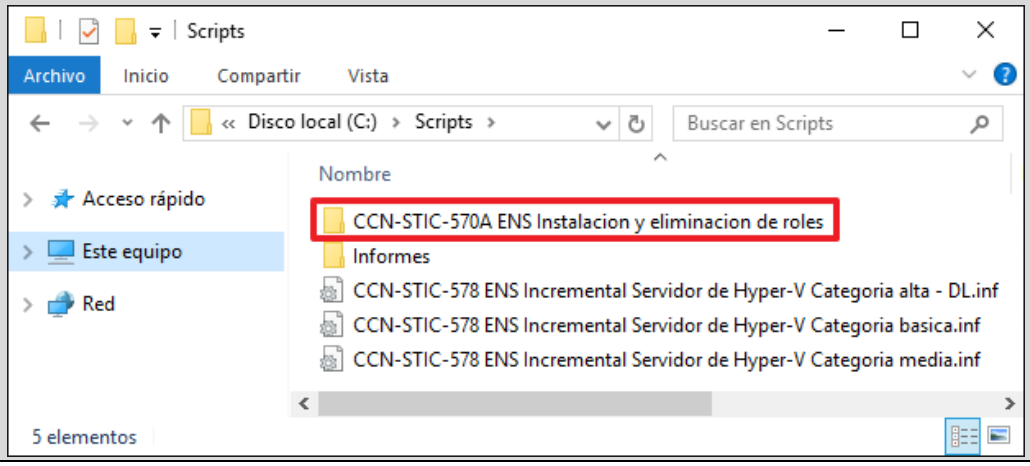
ANEXO A.3.1. PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE HYPER-V SOBRE SERVIDORES WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen servidores de virtualización Hyper-V con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad.

Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría media, deberá realizar las implementaciones según se referencian en el presente anexo.

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

Nota: Si instala el Servidor de Hyper-V por primera vez con la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016 aplicada debe habilitar la instalación remota de roles características y servicios de rol a través de Shell la cual se encuentra deshabilitada por GPO.
En la guía mencionada anteriormente se describe el procedimiento para implementar el objeto GPO que permite la instalación de roles y características. En caso de no disponer de los datos adjuntos a la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016" encontrará una copia de seguridad para poder importar la GPO necesaria en la carpeta "Scripts" adjunta a la presente guía.

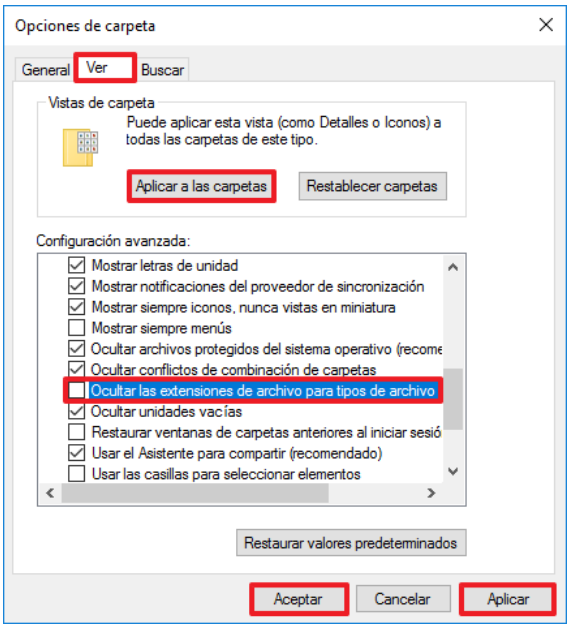
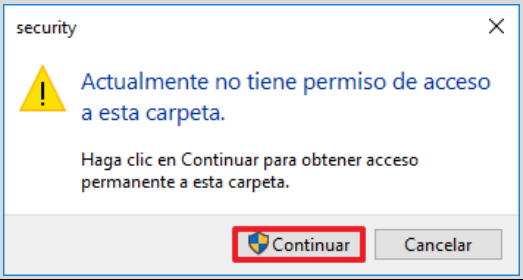


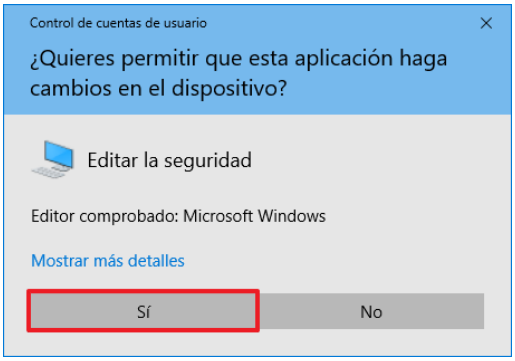
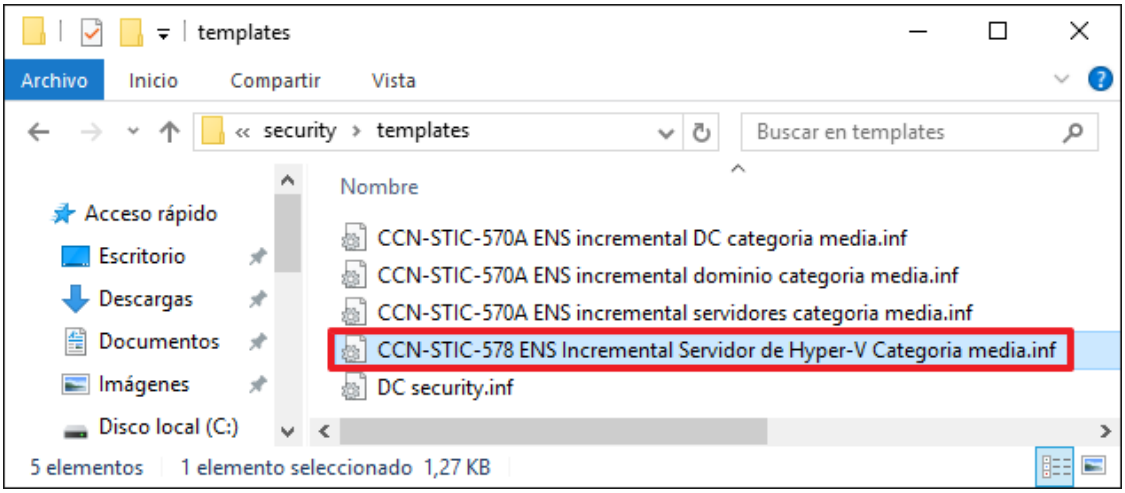
1. PREPARACIÓN DEL DOMINIO

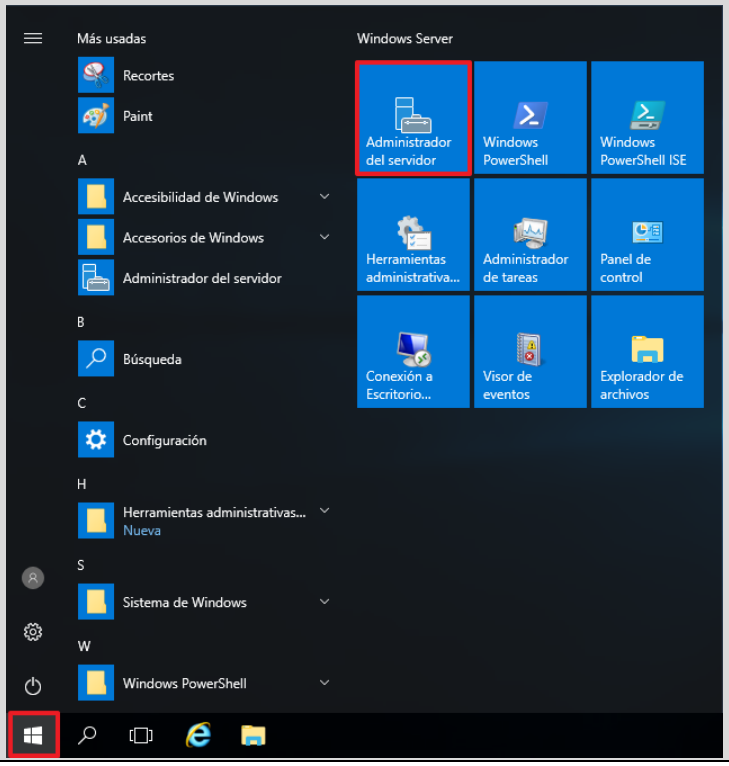
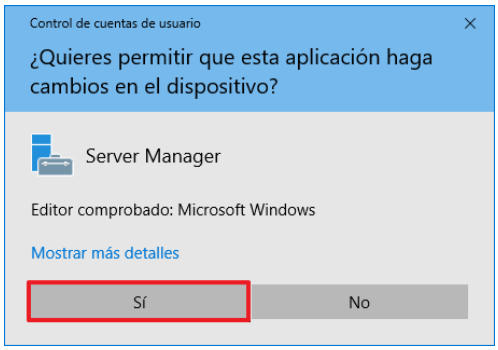
Los pasos que se describen a continuación deberá realizarlos en un Controlador de Dominio del dominio al que pertenece el equipo servidor que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer servidor de Hyper-V que actúe como miembro del dominio. Durante este procedimiento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

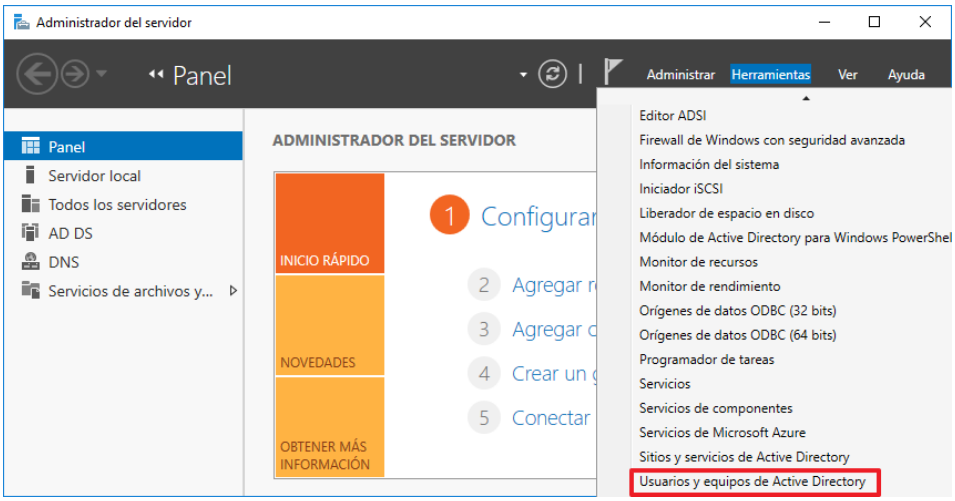
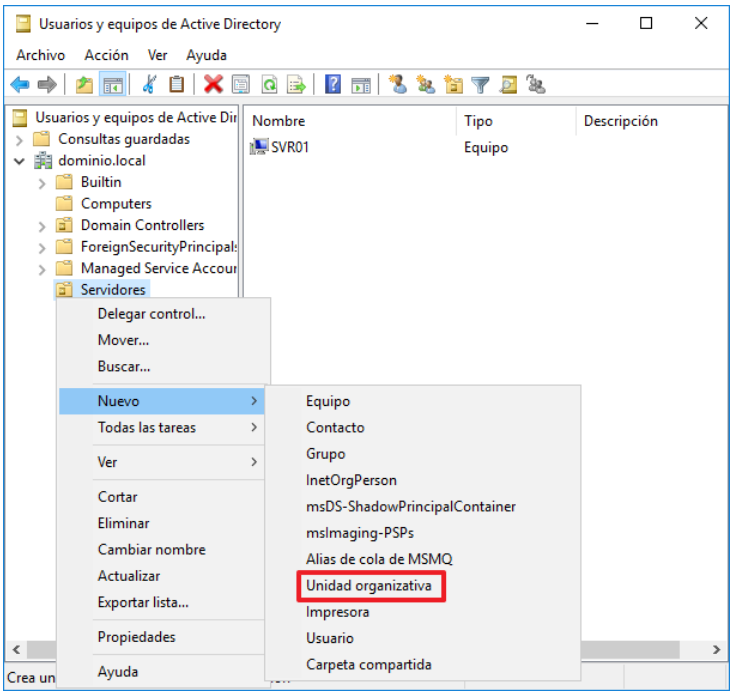
Nota: Esta guía asume que los servidores Controladores del Dominio al que pertenece el equipo servidor de Hyper-V que está asegurando, se les ha aplicado la configuración descrita en la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016". Si no es así, aplique la guía correspondiente al Controlador de Dominio, antes de continuar con la aplicación de ésta.

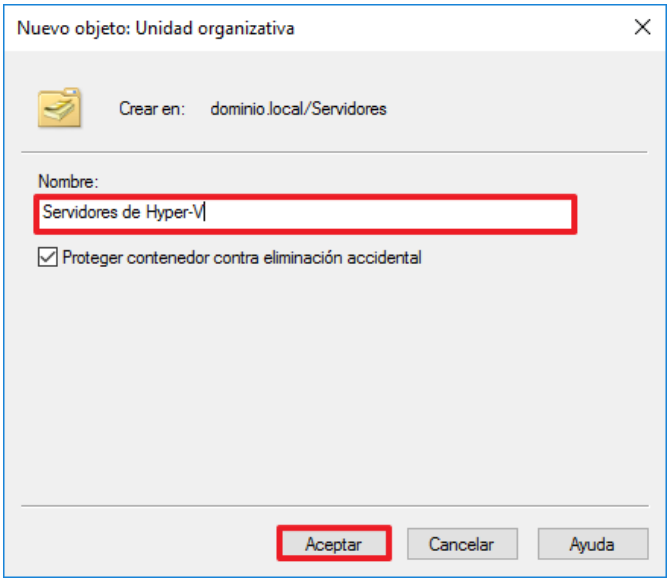
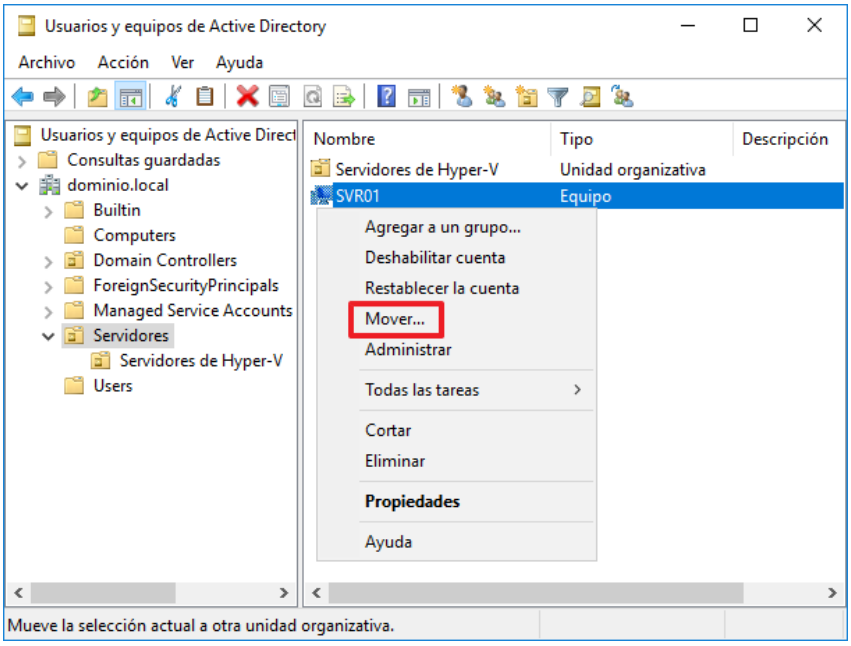
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendrá que editar los scripts para reflejar la nueva ubicación.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.
4.	Si no lo ha hecho anteriormente, configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos.

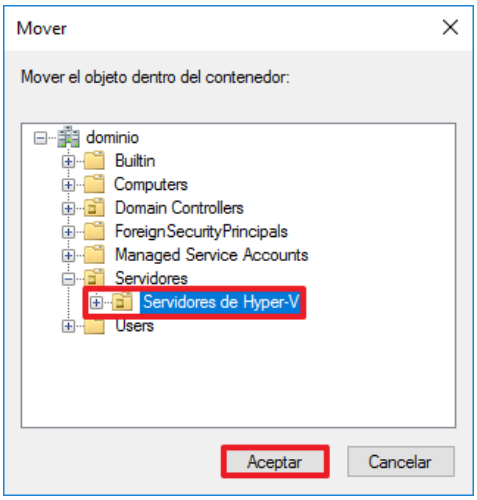
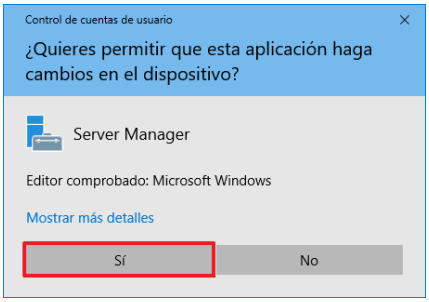
Paso	Descripción
5.	Para configurar el “Explorador de Windows” y que éste muestre las extensiones de todos los archivos, abra una ventana del “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. En la venta emergente, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la imagen.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación “¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?”, y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".
6.	Adicionalmente acceda al directorio “C:\Windows\Security\Templates”. **Nota:** Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón “Continuar” ante la ventana emergente. 

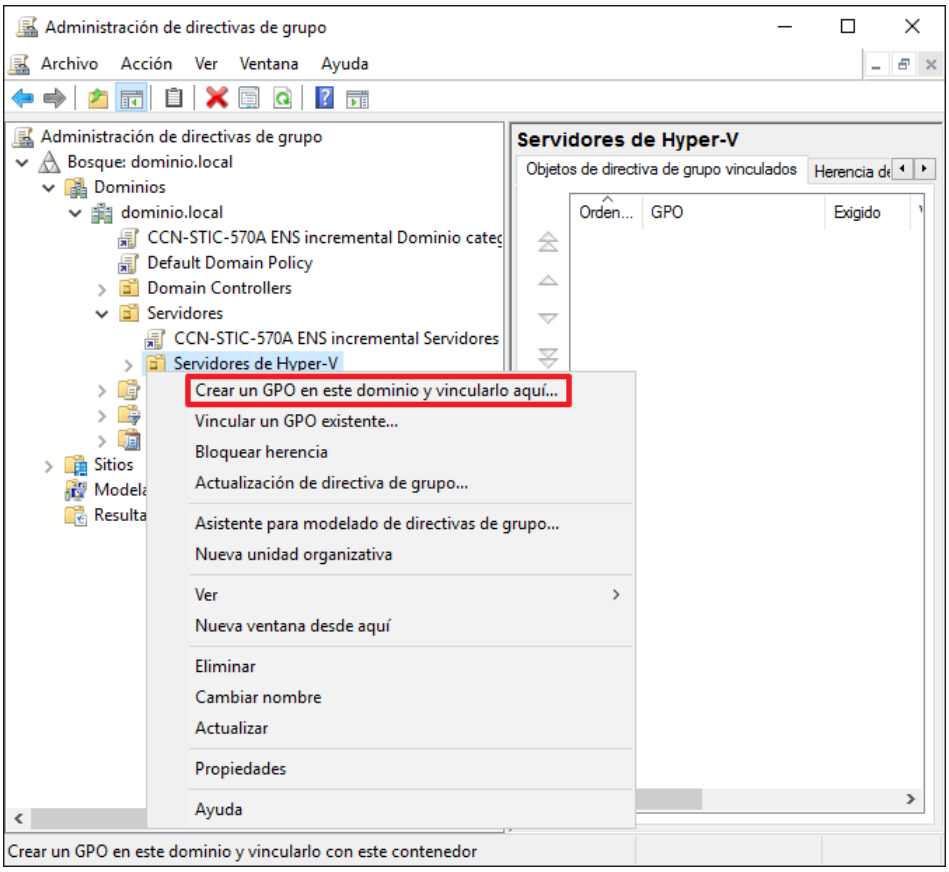
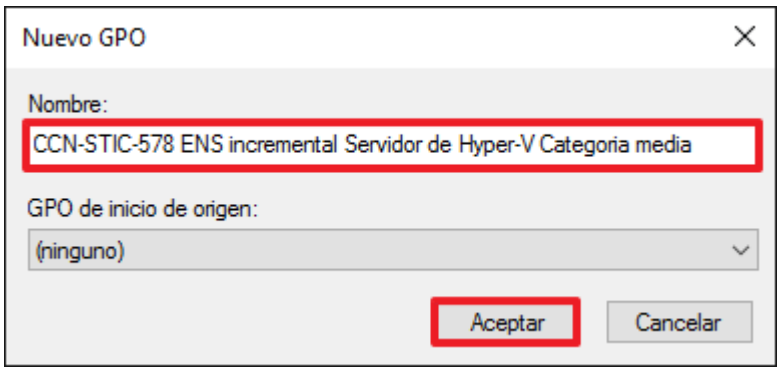
Paso	Descripción
7.	El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar. 
8.	Copie el fichero “CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria media.inf” ubicado en “C:\Scripts” en el directorio “C:\Windows\Security\Templates”. 

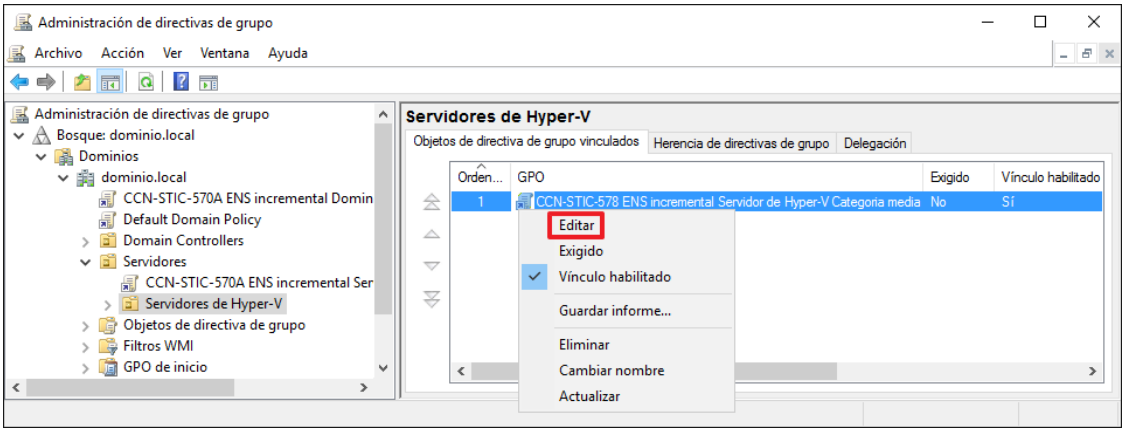
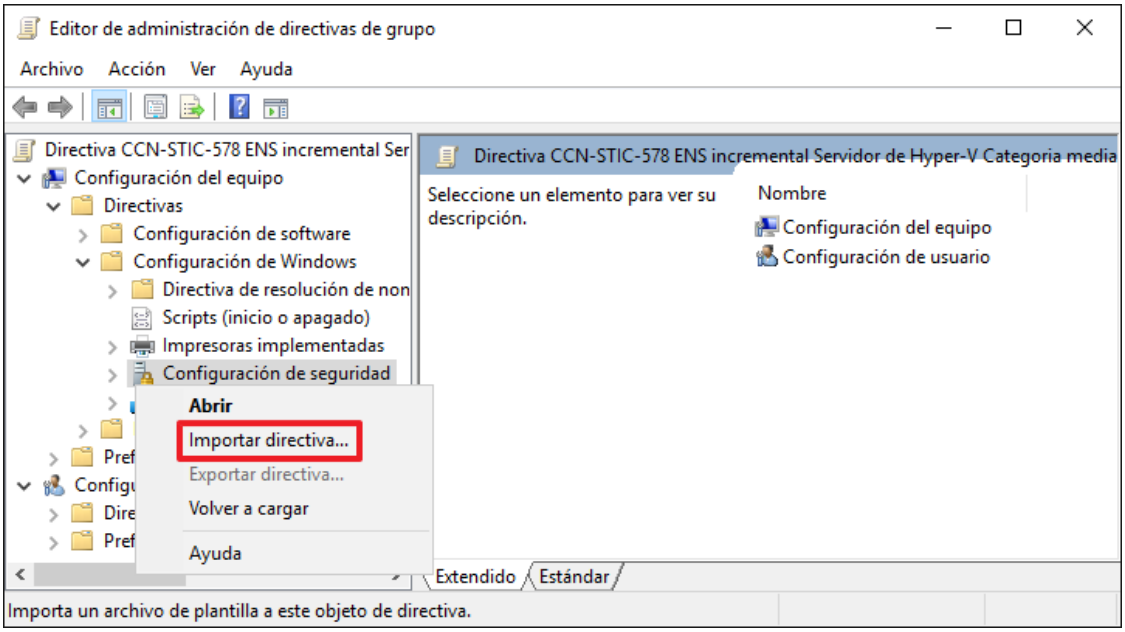
Paso	Descripción
9.	A continuación, deberá crear la unidad organizativa "Servidores de Hyper-V". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente.  **Nota:** Por defecto el "Administrador del servidor" se inicia cuando un usuario inicia sesión en el equipo. Si no se encuentra vinculado a la barrada de tareas podrá acceder a él en la ruta **"Inicio → Administrador del servidor"**. 
10.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 

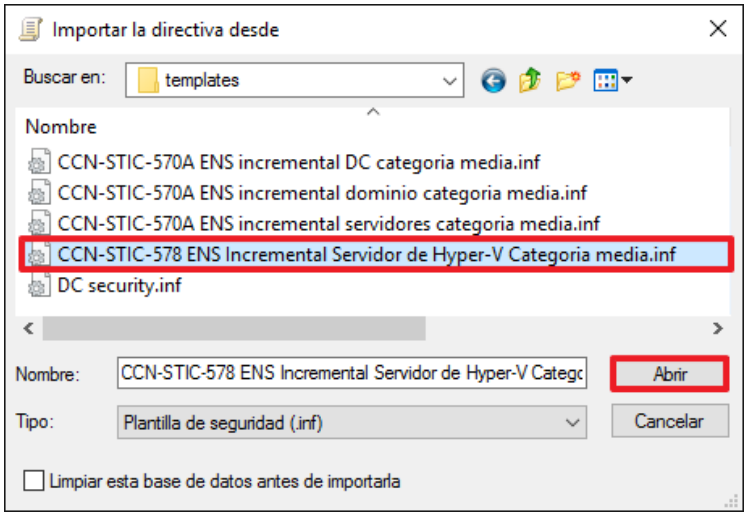
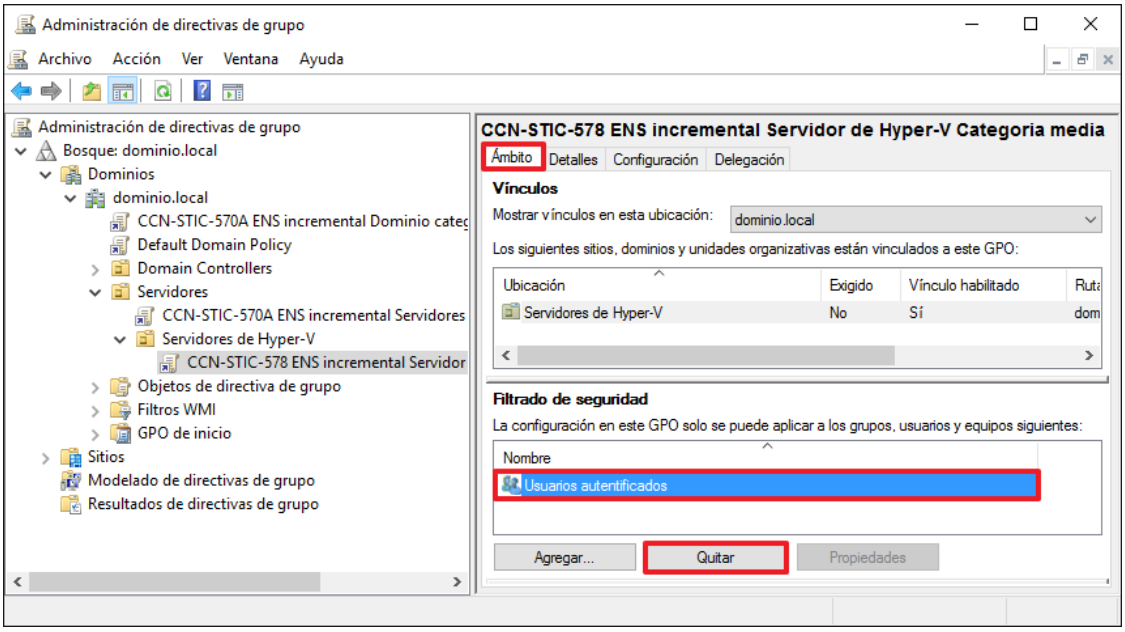
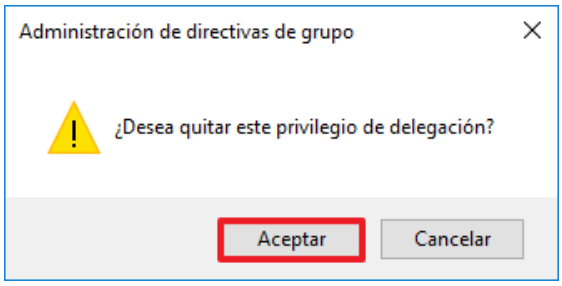
Paso	Descripción
11.	Inicie la herramienta “Usuarios y equipos Active Directory”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Usuarios y equipos de Active Directory”**. 
12.	En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo **“<<dominio>> → <<unidad organizativa>>”**, y desplegando el menú contextual con el botón derecho, seleccione la opción **“Nuevo → Unidad organizativa”**.  **Nota:** En este ejemplo, la unidad organizativa de servidores se encuentra en el nodo **“dominio.local → Servidores”**.

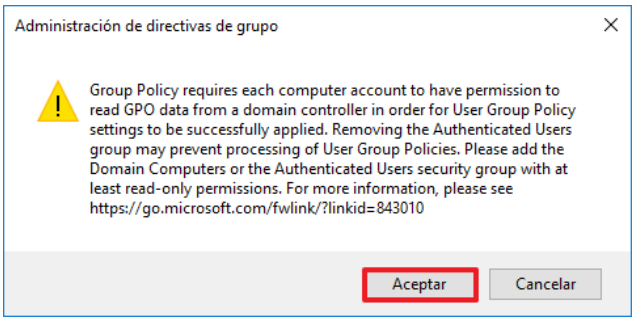
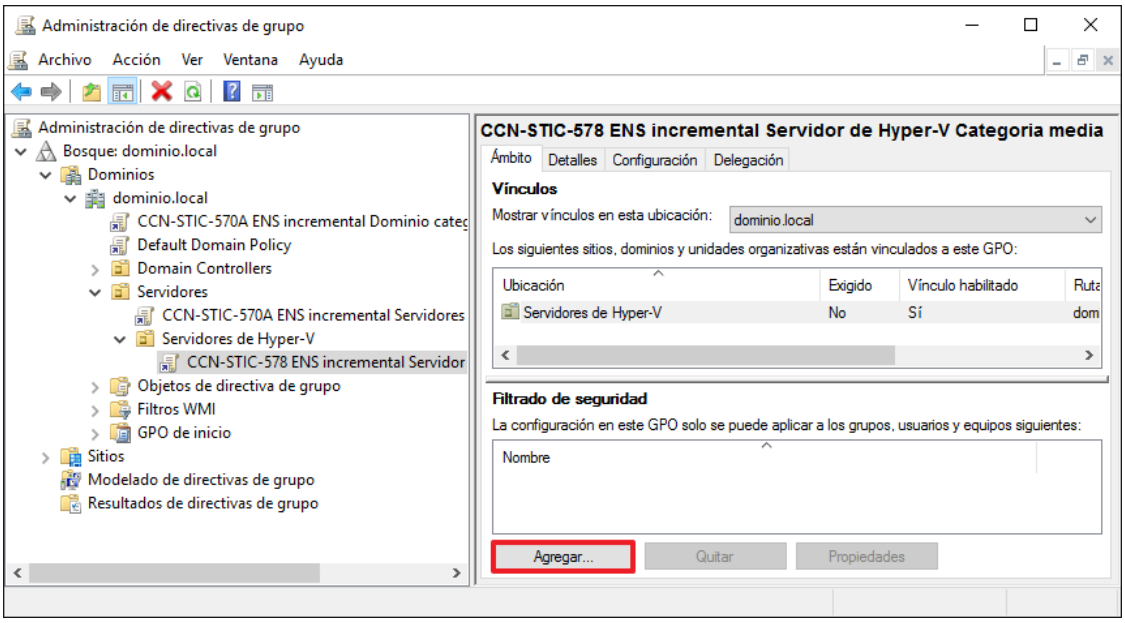
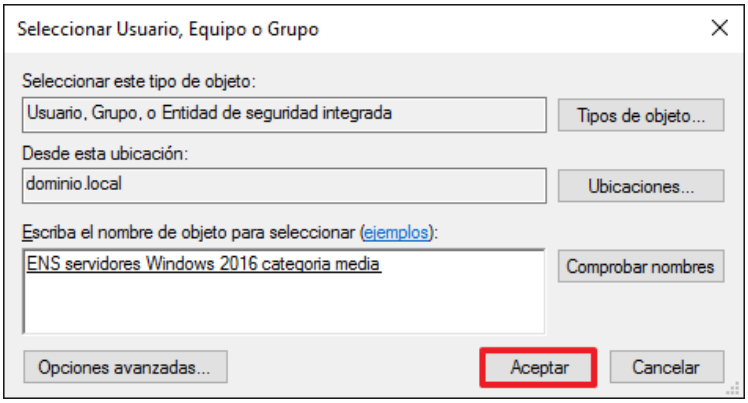
Paso	Descripción
13.	Introduzca el nombre “Servidores de Hyper-V” tal y como se muestra en la imagen y pulse sobre “Aceptar”. 
14.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores de virtualización a la unidad organizativa “Servidores de Hyper-V”. Para ello, haga clic con el botón derecho sobre el equipo que desee reubicar y seleccione la opción del menú contextual “Mover...”. 

Paso	Descripción
15.	A continuación, seleccione la unidad organizativa “Servidores de Hyper-V” y pulse “Aceptar”. 
16.	Cierre la herramienta “Usuarios y equipos de Active Directory”.
17.	A continuación, deberá crear la GPO "CCN-STIC-578 ENS incremental Servidor de Hyper-V categoria media". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 
18.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
19.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administración de directivas de grupo”.** 

Paso	Descripción
20.	A continuación, despliegue el nodo **"Bosque: <<nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores de Hyper-V"**. **Nota:** En este ejemplo el nombre de la unidad organizativa donde se encuentran todos los servidores que implementan este rol, "Servidores de Hyper-V".
21.	Pulse con el botón derecho sobre la unidad organizativa "Servidores de Hyper-V" y seleccione "Crear un GPO en este dominio y vincularlo aquí…". 
22.	Introduzca el nombre del objeto GPO, "CCN-STIC-578 ENS incremental Servidor de Hyper-V Categoria media" y haga clic en el botón "Aceptar". 

Paso	Descripción
23.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción "Editar". 
24.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad"**.
25.	Pulse con el botón derecho sobre "Configuración de seguridad" y seleccione la opción "Importar directiva…". 

Paso	Descripción
26.	Seleccione de la ruta "C:\Windows\Security\Templates" el fichero "CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria media.inf" y pulse el botón "Abrir". 
27.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
28.	Seleccione la nueva política de grupo configurada y vaya a la pestaña "Ámbito" que se encuentra en el panel derecho. En la opción "Filtrado de seguridad", seleccione "Usuarios autentificados" y pulse la opción "Quitar". 
29.	Pulse "Aceptar" ante el mensaje emergente "¿Desea quitar este privilegio de delegación?". 

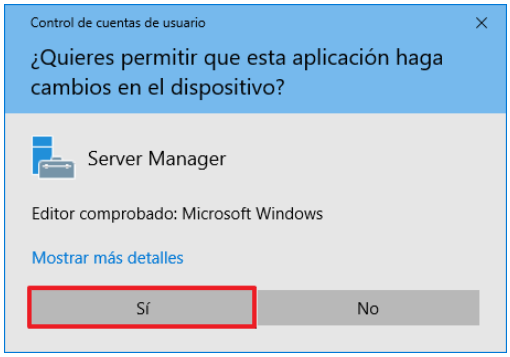
Paso	Descripción
30.	Pulse de nuevo “Aceptar” ante el mensaje de advertencia emergente. 
31.	A continuación, pulse el botón “Agregar…”. 
32.	Introduzca como nombre “ENS Servidores Windows 2016 categoria media”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A Implementación del ENS en Windows Server 2016”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado, deberá adaptar estos pasos a las necesidades de su organización.

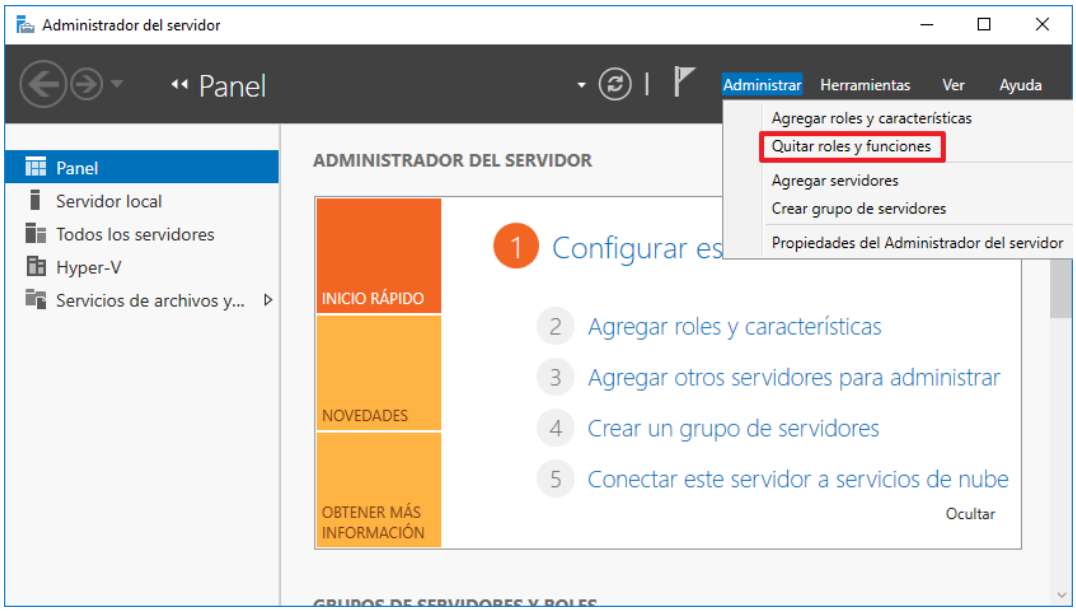
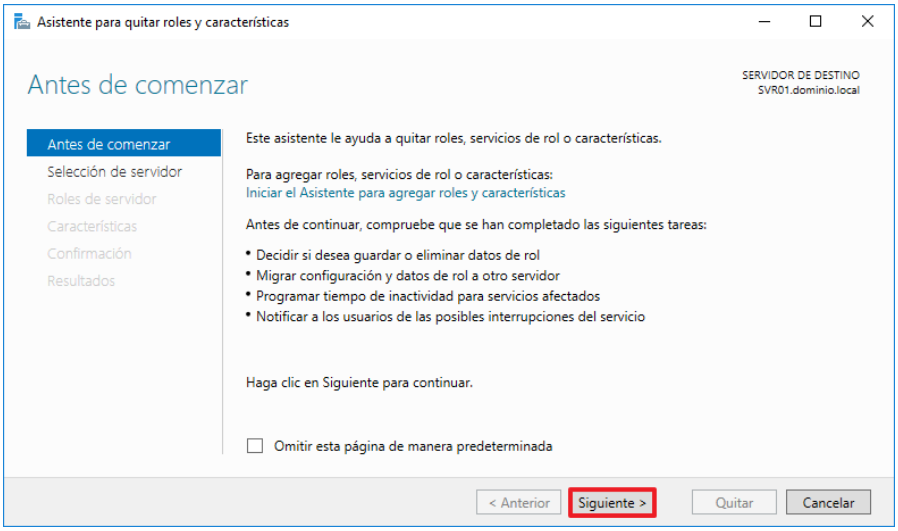
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

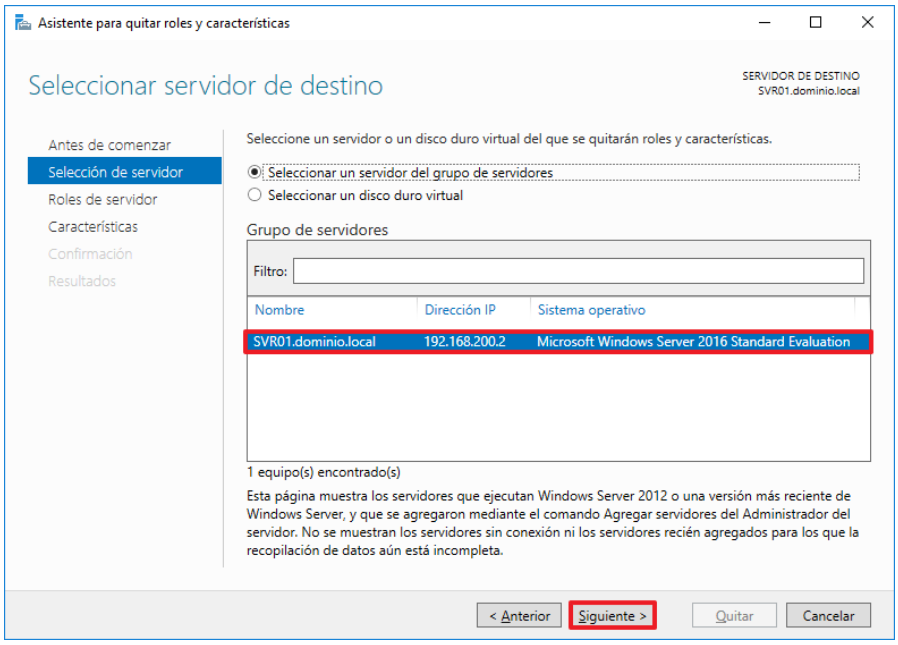
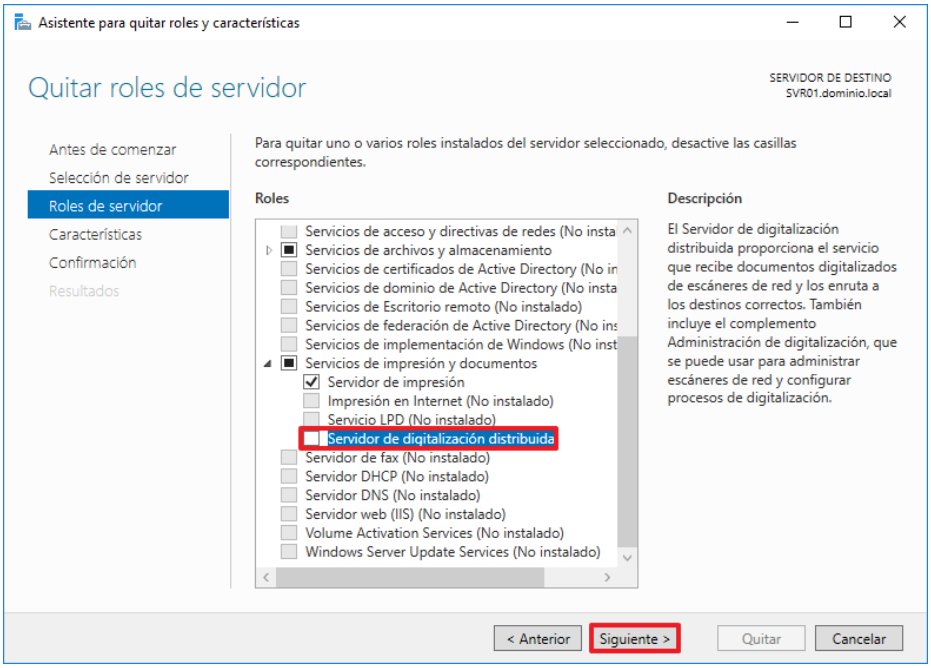
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

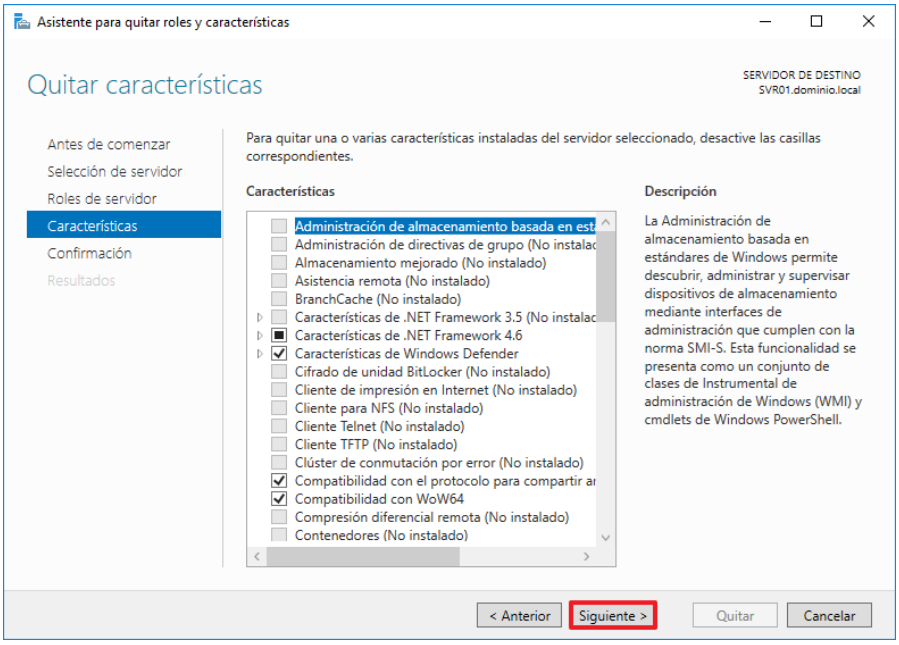
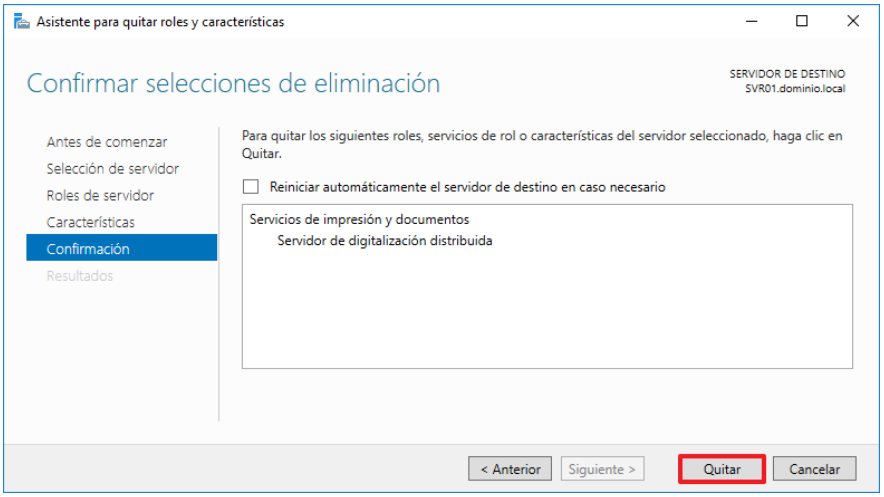
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

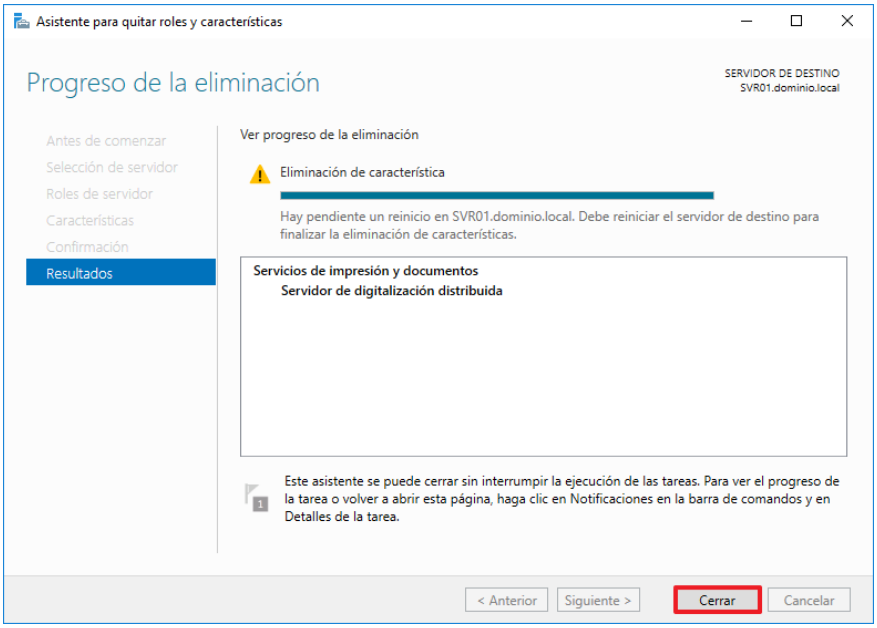
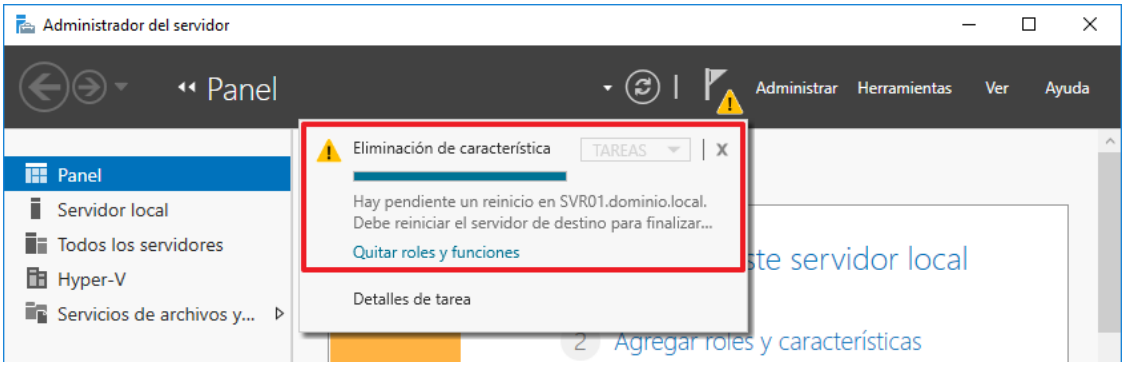
En el procedimiento que se describe a continuación, a modo de ejemplo, desinstala un rol que actualmente no está siendo utilizado por el Servidor de Hyper-V.

Paso	Descripción
33.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
34.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
35.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 

Paso	Descripción
36.	A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”. 
37.	Se lanzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 

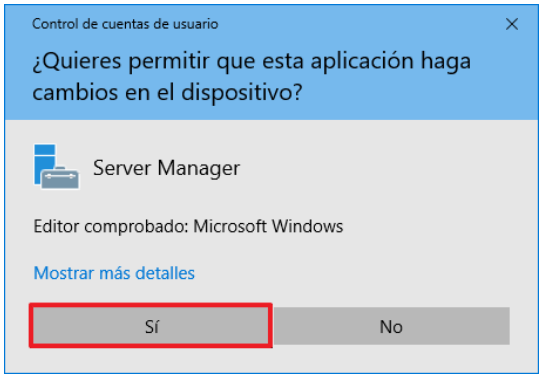
Paso	Descripción
38.	Seleccione el servidor sobre el cual desea eliminar un rol o característica y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “SVR01”.
39.	En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se desinstala el rol “Servidor de digitalización distribuida”.

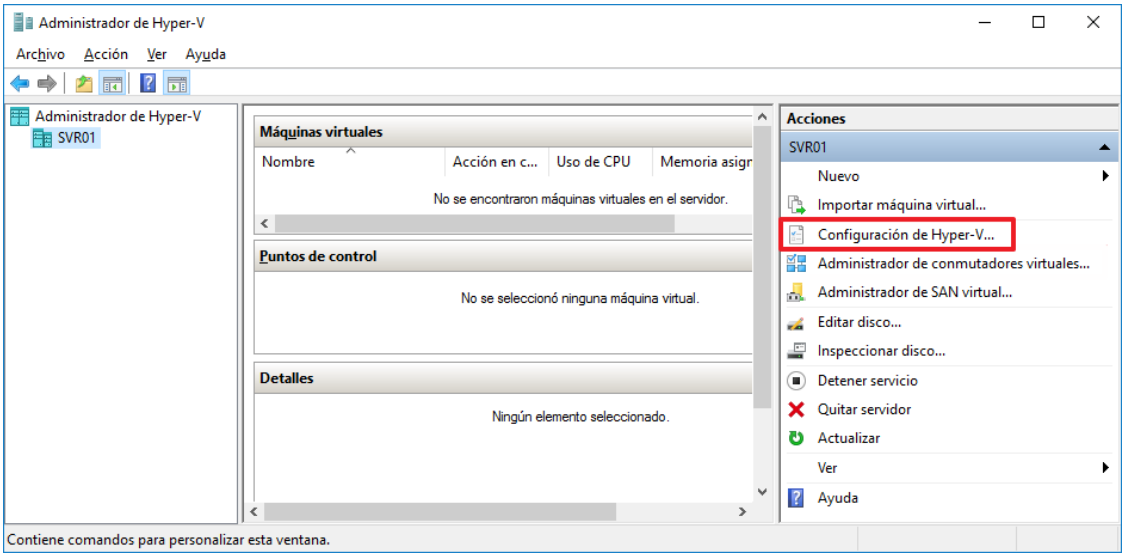
Paso	Descripción
40.	En la ventana de características pulse el botón “Siguiente >”. En este ejemplo no se desinstala ninguna característica adicional. 
41.	En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso. 

Paso	Descripción
42.	El proceso comenzará y una vez finalizado, y si todo ha ido bien bastará con pulsar sobre “Cerrar” para finalizar la desinstalación. 
43.	En caso de ser necesario el servidor requerirá un reinicio para finalizar la configuración. El “Administrador del servidor” mostrará una advertencia acerca de la necesidad de dicho reinicio. 

2.2. CONFIGURACIÓN GENERAL DE HYPER-V

La gestión de la configuración de Hyper-V constituye una importante tarea de administración debido a que permite establecer o modificar configuraciones que afectan a la funcionalidad del servicio de virtualización

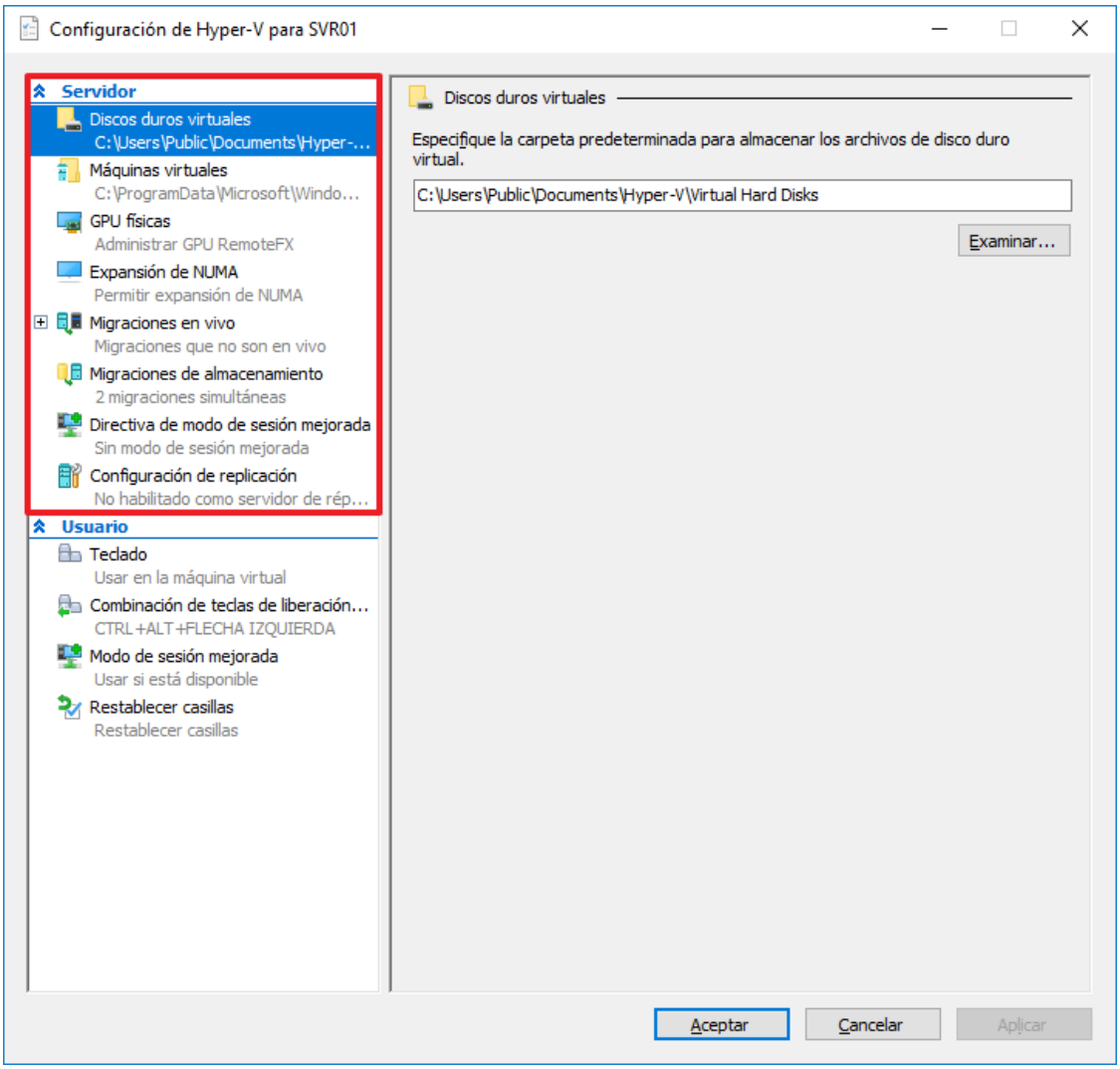
Paso	Descripción
44.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
45.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
46.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 

Paso	Descripción
47.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
48.	Dentro de la consola emergente seleccione el servidor de Hyper-V instalado en el servidor y a continuación en el panel de "Acciones" seleccione la opción "Configuración de Hyper-V…". 
49.	En los siguientes apartados se definirán las configuraciones dedicadas al propio servidor de Hyper-V y aquellas configuraciones que afectan a la experiencia de usuario con el servicio de virtualización.

2.2.1. CONFIGURACIÓN DEL SERVIDOR

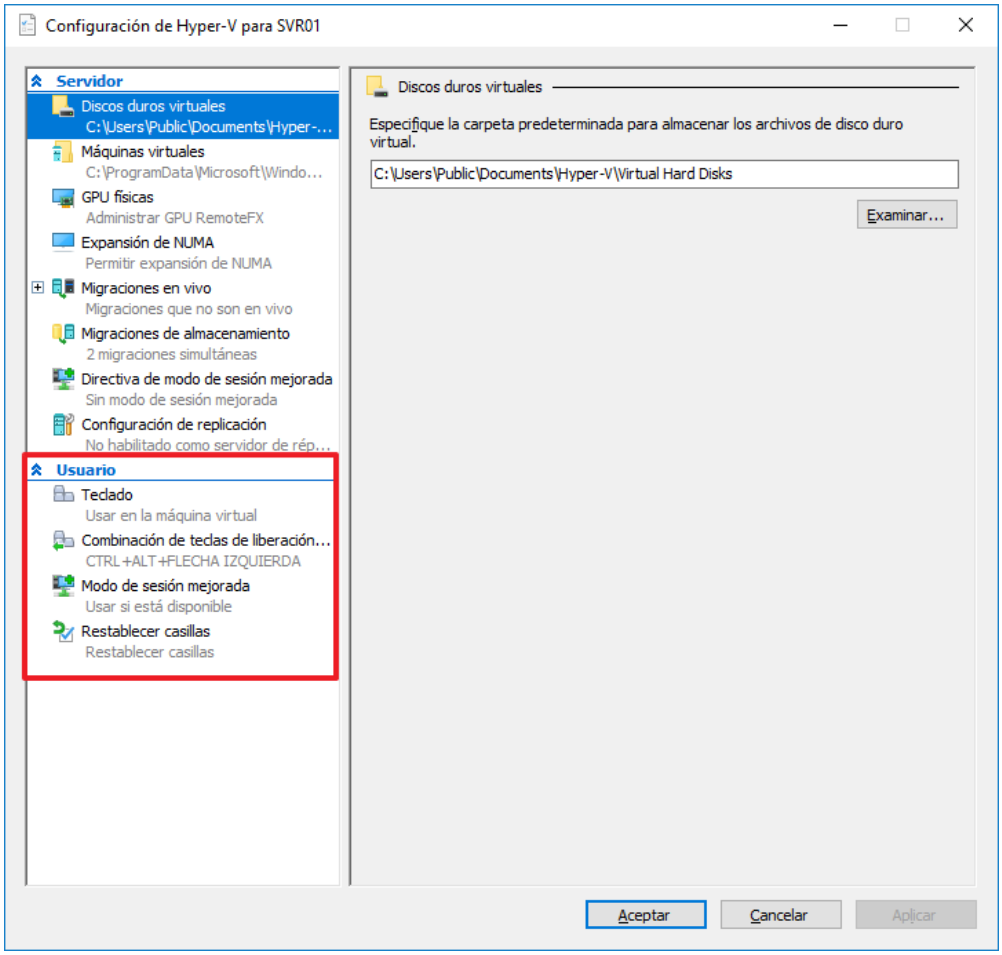
Este apartado define la configuración dedicada al servidor de Hyper-V la cual permite gestionar y administras las configuraciones más generales del servicio de virtualización.

Paso	Descripción
50.	Dentro de la ventana "Configuración de Hyper-V para <<su servidor>>" acceda al apartado denominado "Servidor".

Paso	Descripción
51.	Dentro de este apartado defina las configuraciones necesarias que permitan mejorar o establecer configuraciones de uso para el servidor Hyper-V. 
52.	Dentro de estas configuraciones que es posible deberá prestar especial atención a las siguientes: – **Discos duros virtuales:** permite definir la ubicación por defecto de los discos de las máquinas virtuales. – **Máquinas virtuales:** permite definir la ubicación por defecto de los ficheros que componen las máquinas virtuales. – **Migraciones en vivo:** permite realizar migraciones de máquinas virtuales mientras éstas se encuentran en uso. – **Configuración de replicación:** esta configuración permite disponer de una copia casi instantánea en otro servidor de Hyper-V.

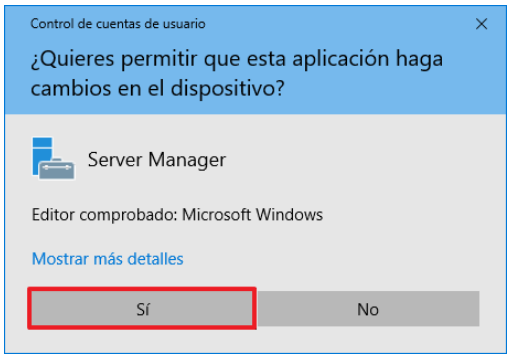
2.2.2. CONFIGURACIÓN DEL USUARIO

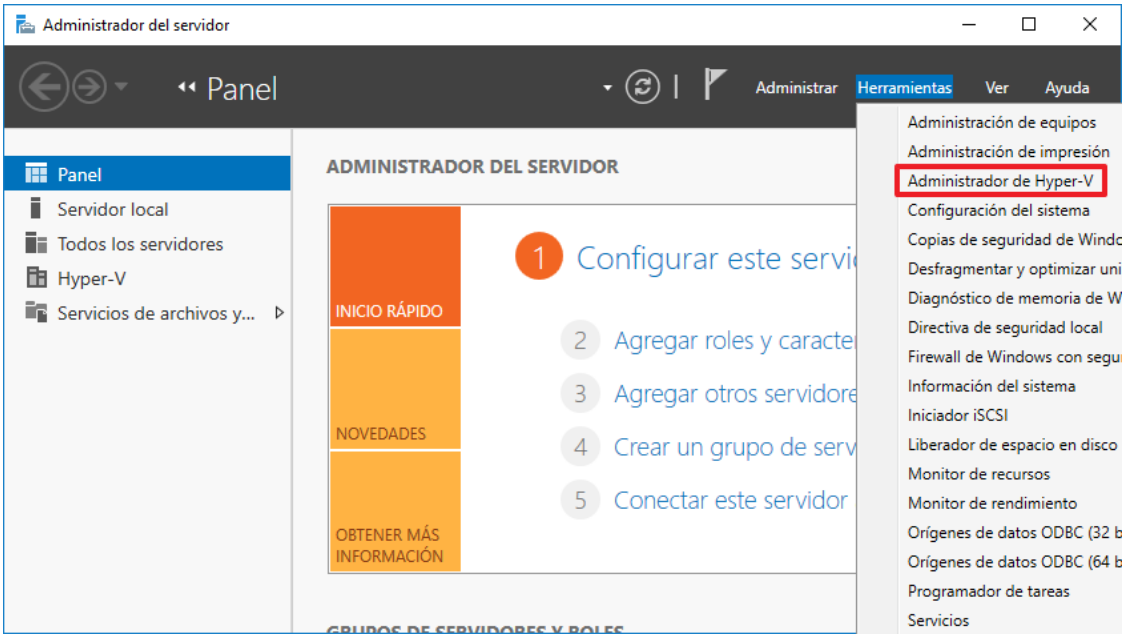
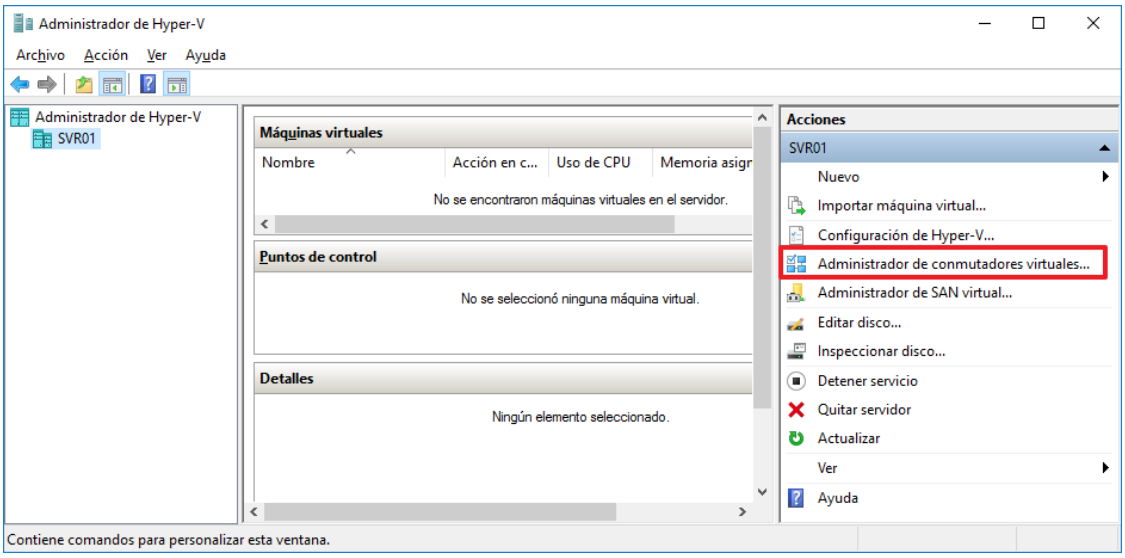
Este apartado define la configuración dedicada al usuario en su interacción con el servicio de virtualización.

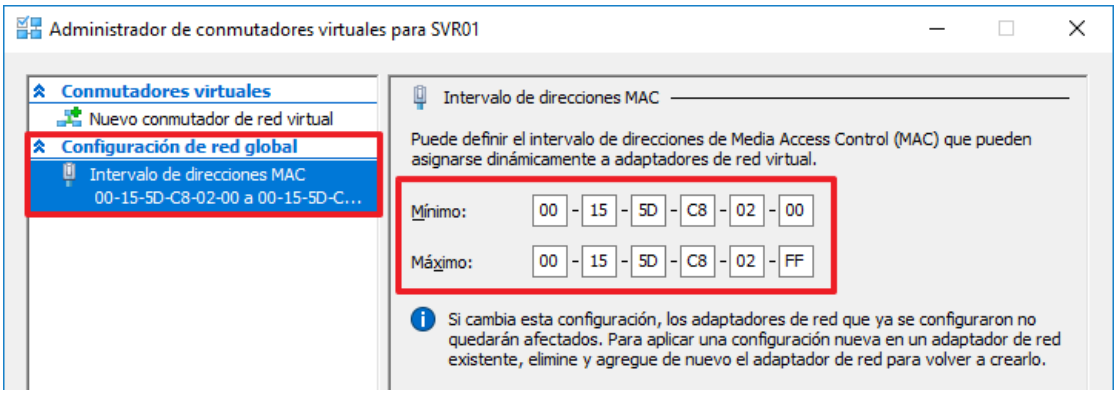
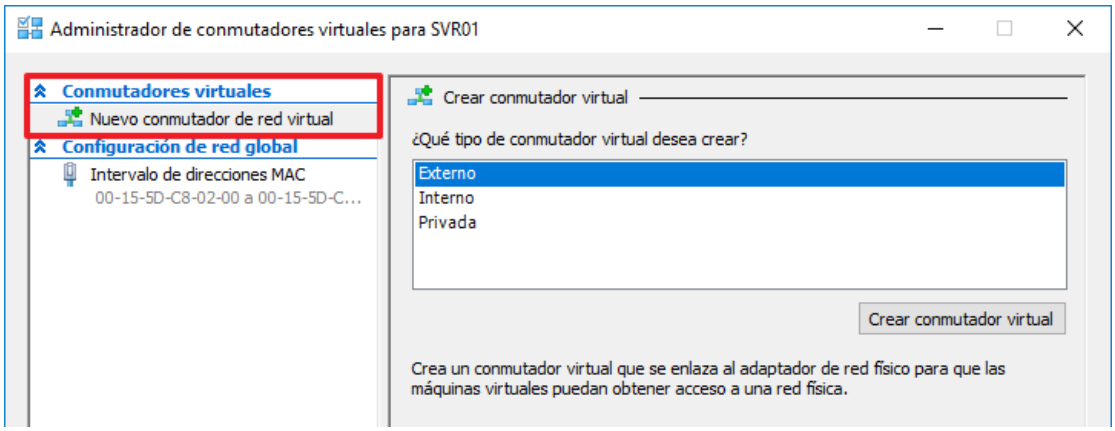
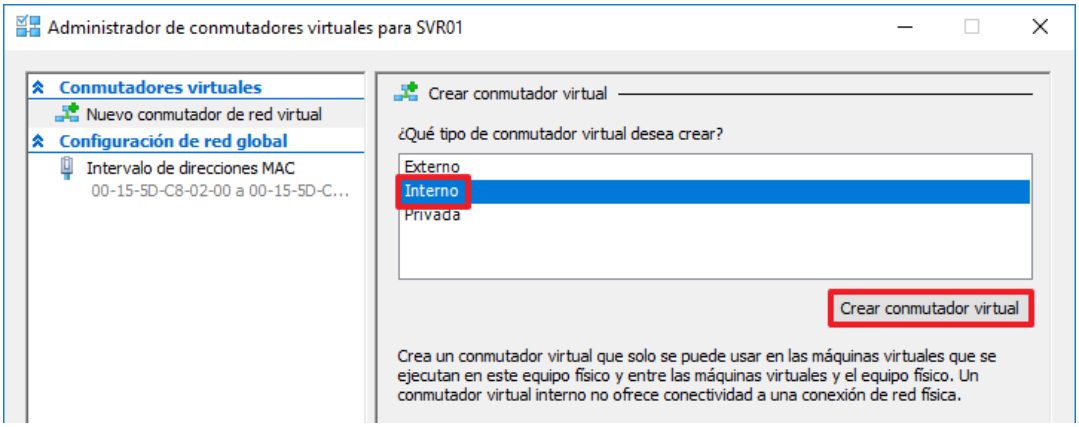
Paso	Descripción
53.	Dentro de la ventana “Configuración de Hyper-V para <<su servidor>>” acceda al apartado denominado “Usuario”.
54.	Dentro de este apartado defina las configuraciones necesarias que permitan mejorar o establecer configuraciones de uso para el servidor Hyper-V. 
55.	Las configuraciones de las que dispone este apartado son las siguientes: – **Teclado:** permite establecer cómo se comportan las combinaciones de teclado en las máquinas virtuales. – **Combinación de teclas de liberación del mouse:** define la combinación de teclas a utilizar para “liberar” el ratón de la máquina virtual sobre la que se está trabajando. – **Modo de sesión mejorada:** permite el redireccionamiento de dispositivos y recursos locales (copiar y pegar) de equipos que ejecutan una conexión con una máquina virtual. – **Reestablecer casillas:** permite volver a un estado de “recién instalado” en el que Hyper-V muestra mensajes de confirmación que han sido ya omitidos.

2.3. GESTIÓN DE CONMUTADORES VIRTUALES

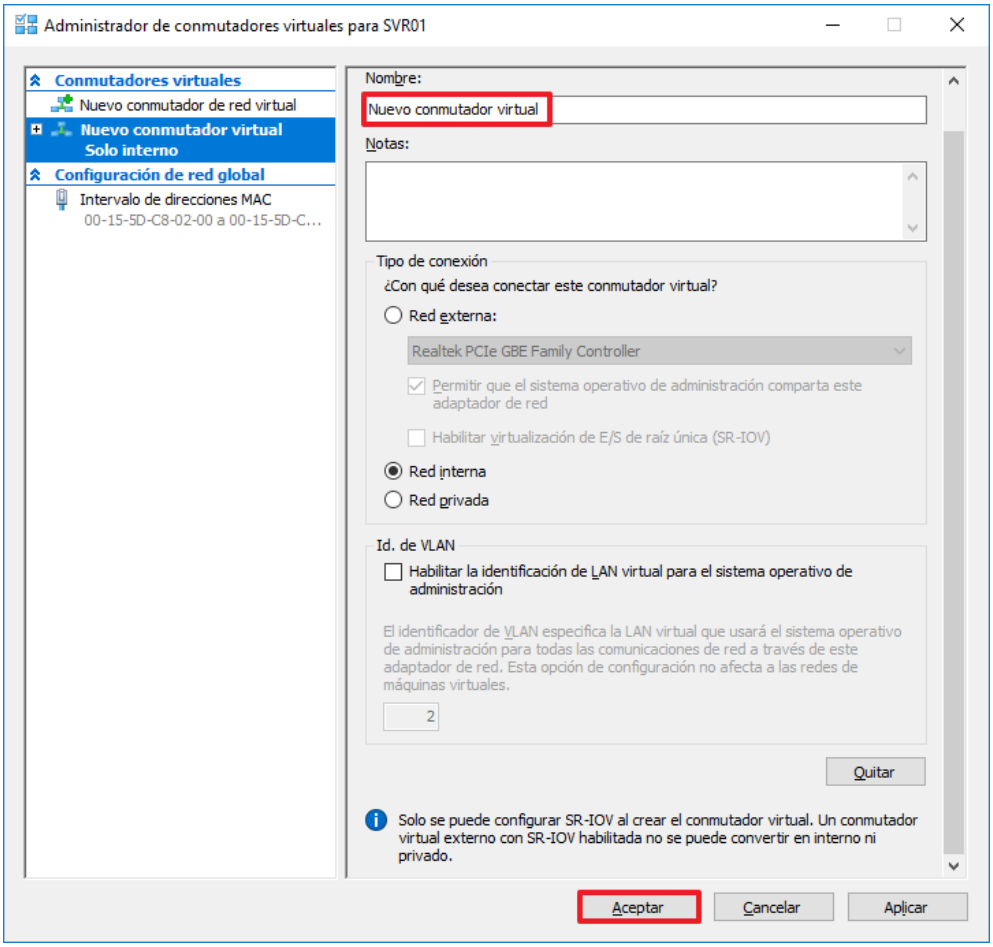
Dentro del servidor de Hyper-V es importante realizar una correcta gestión de las redes disponibles con el fin de determinar cómo se comporta la red de las diferentes máquinas virtuales y permitir establecer o denegar comunicaciones según sea necesario.

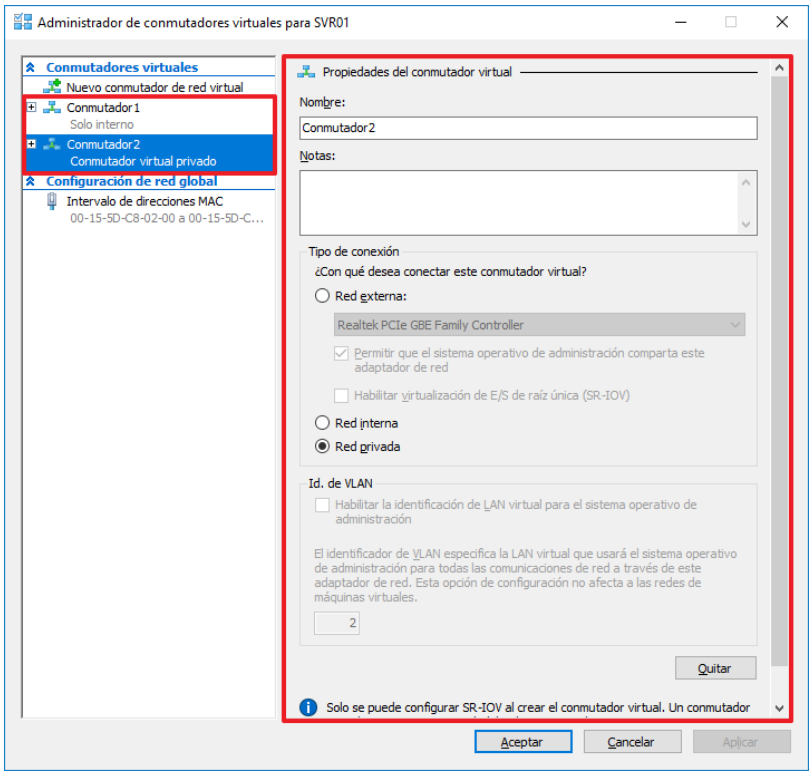
Paso	Descripción
56.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
57.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
58.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 

Paso	Descripción
59.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
60.	Dentro de la consola emergente seleccione el servidor de Hyper-V instalado en el servidor y a continuación en el panel de "Acciones" seleccione la opción "Administrador de conmutadores virtuales". 

Paso	Descripción
61.	En la ventana emergente “Administrador de conmutadores virtuales para <<su servidor>>” dentro del apartado “Configuración de red global” seleccione “Intervalo de direcciones MAC”. Establezca el intervalo mínimo y máximo de direcciones MAC que pueden asignarse a los adaptadores de red virtuales.  **Nota:** Deberá tener en cuenta las especificaciones necesarias para establecer el direccionamiento MAC adecuado. En este ejemplo, se establece por defecto.
62.	A continuación, seleccione dentro del apartado “Conmutadores virtuales” la opción “Nuevo conmutador de red virtual”. 
63.	Seleccione entonces el tipo de conmutador virtual de red deseado. Deberá tener en consideración las necesidades de su organización en el momento de crear dichos adaptadores virtuales de red.  **Nota:** Para este ejemplo se crea un conmutador de red “Interno”

Paso	Descripción
64.	Aparecerá otra ventana en la que se mostrarán las opciones disponibles sobre el adaptador de red creado. Establezca un nombre y si lo desea una descripción. Por último, pulse sobre “Aceptar”.

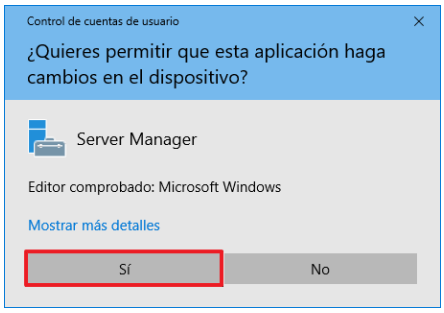
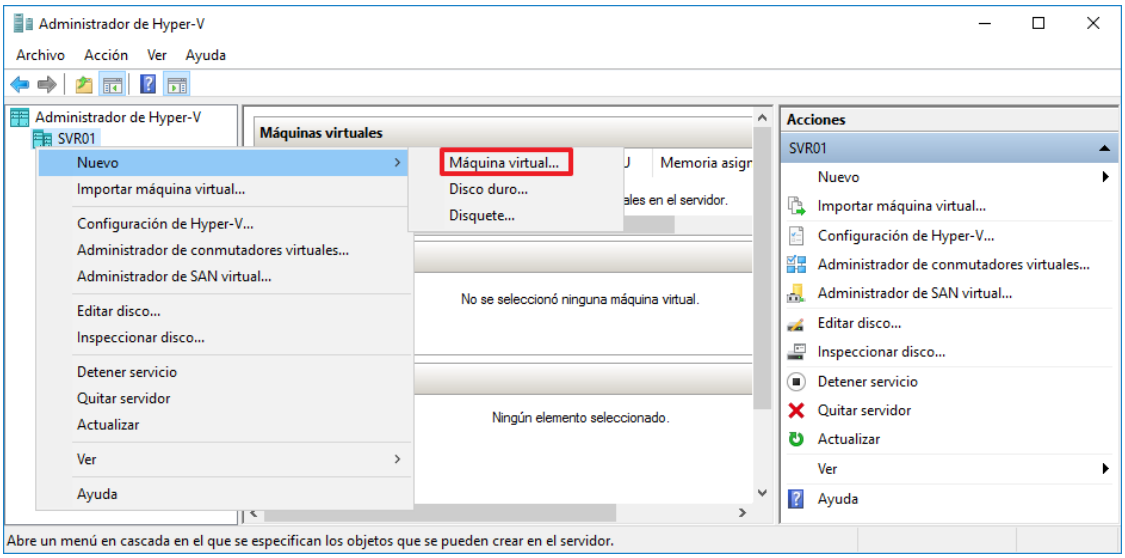


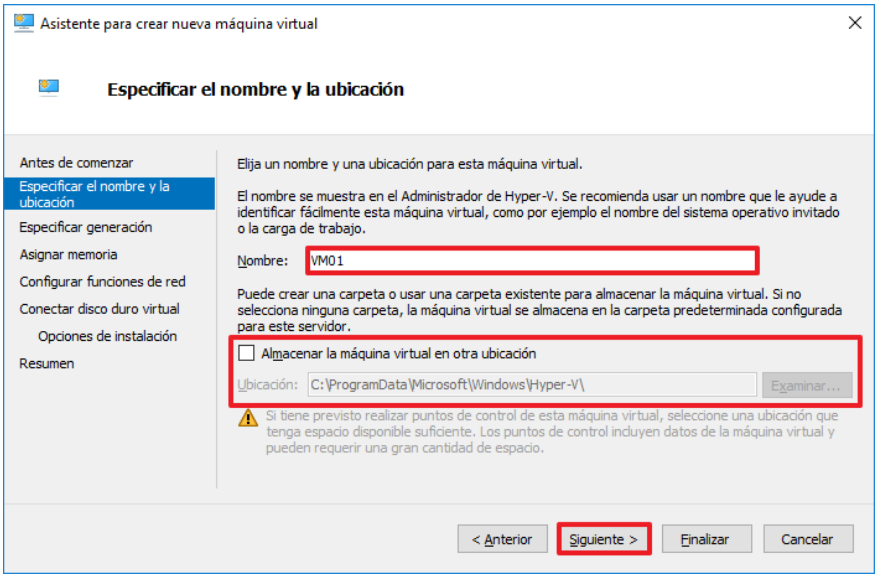
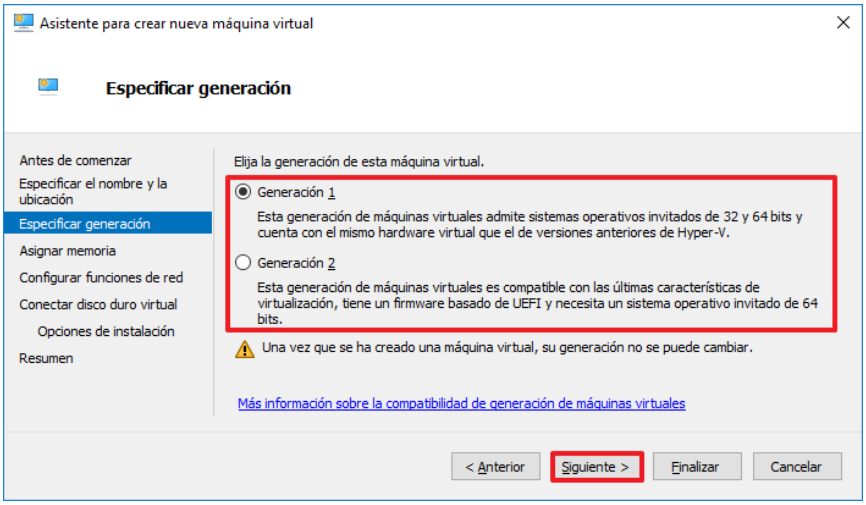
Paso	Descripción
65.	Podrá realizar una gestión sobre los conmutadores creados pulsando sobre cada uno de ellos y modificando la configuración que ya poseen. Del mismo modo es posible eliminar conmutadores que ya no sean requeridos haciendo uso del botón “Quitar”. 

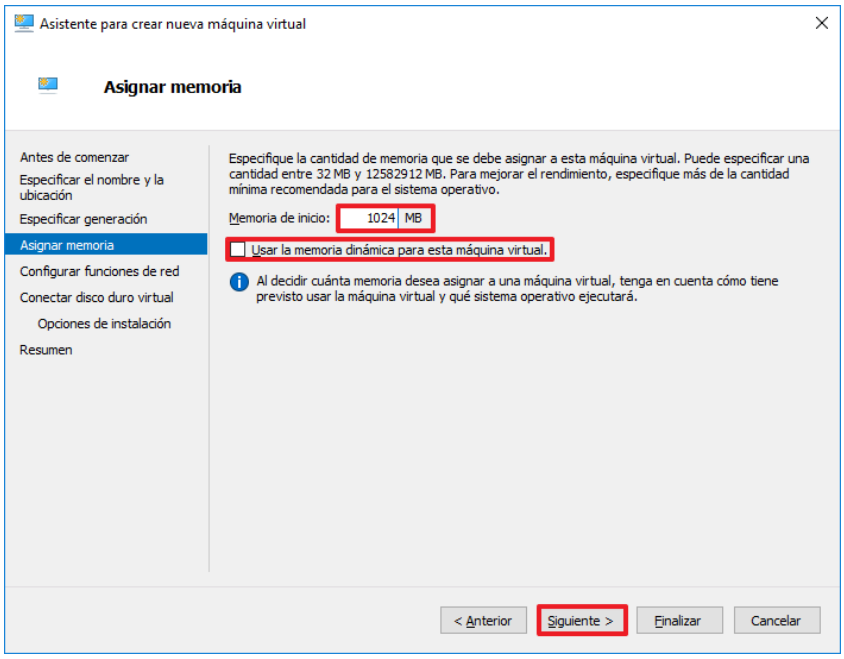
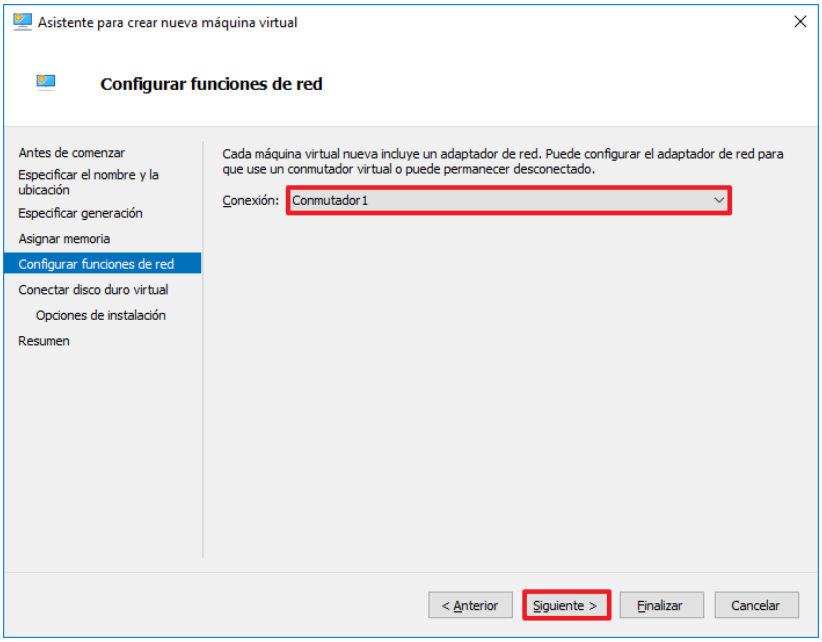
2.4. GESTIÓN DE MÁQUINAS VIRTUALES

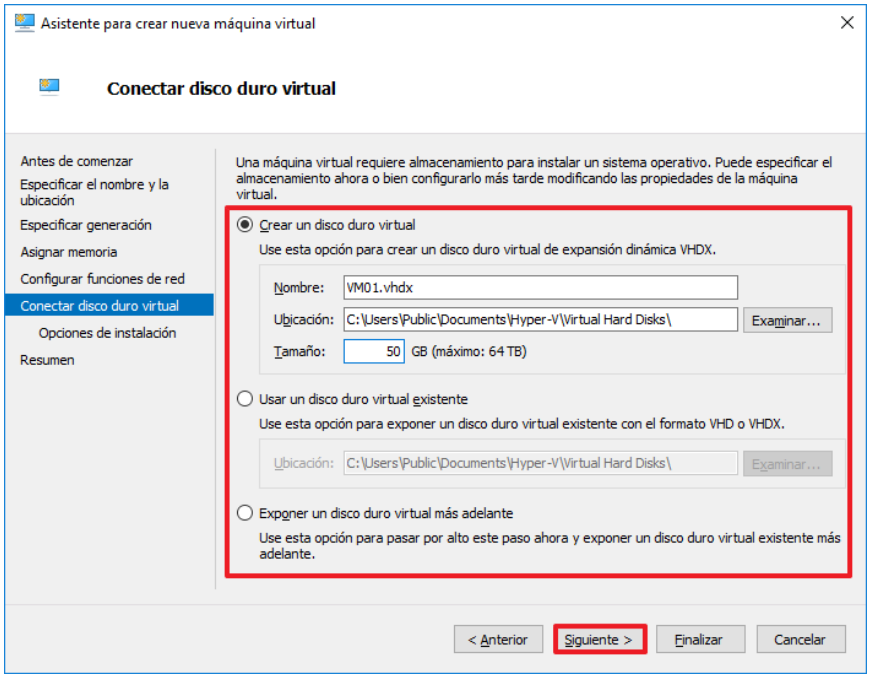
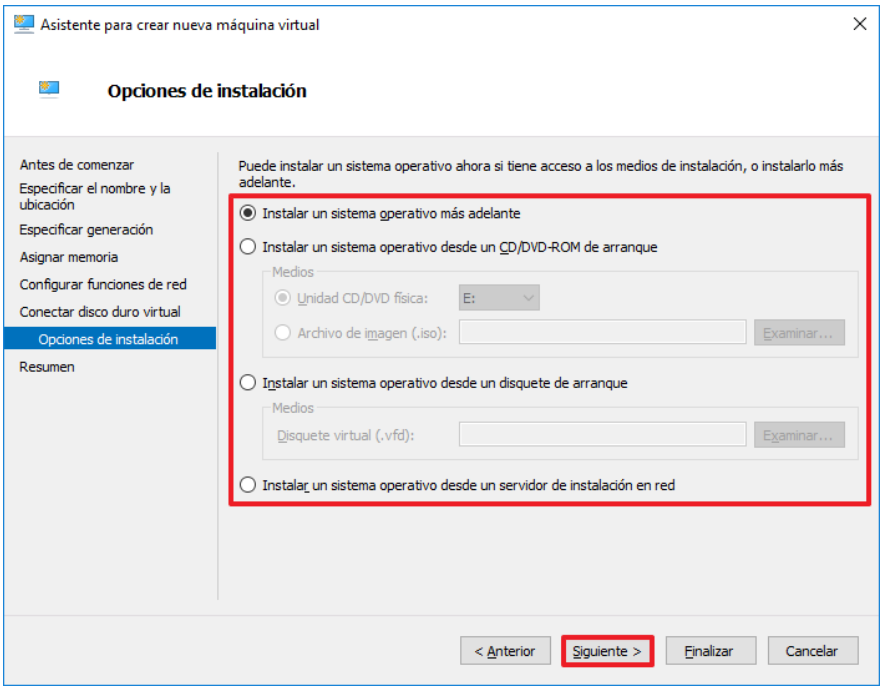
Otra de las tareas esenciales es la creación de máquinas virtuales ya que éstas son las que ofrecen el servicio propiamente dicho. En este apartado se realiza un ejemplo de creación y configuración de una máquina virtual.

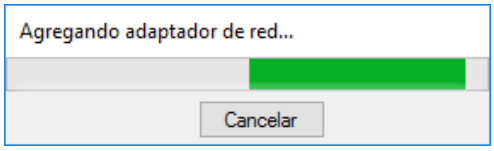
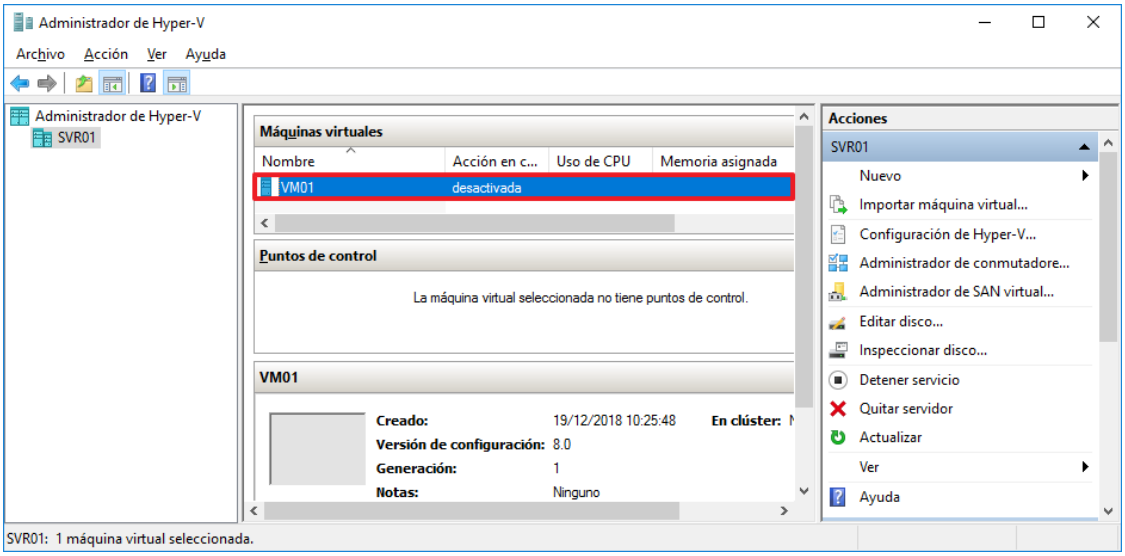
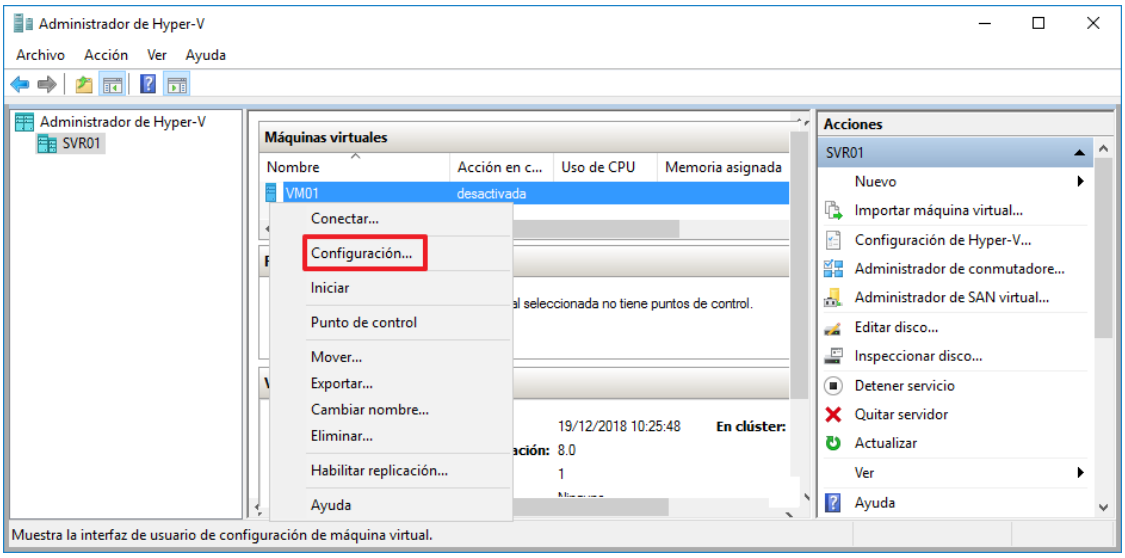
Paso	Descripción
66.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
67.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.

Paso	Descripción
68.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
69.	Inicie la herramienta “Administrador de Hyper-V”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administrador de Hyper-V”**. 
70.	Dentro de la consola emergente seleccione el servidor de Hyper-V con el botón derecho y seleccione la opción del menú contextual **“Nuevo → Máquina virtual…”**.  **Nota:** En este ejemplo el servidor de denomina “SVR01”. Deberá adaptar estos pasos a las configuraciones de su organización.
71.	Aparecerá el asistente para la creación de máquinas virtuales. En la ventana “Antes de comenzar” pulse “Siguiente >”.

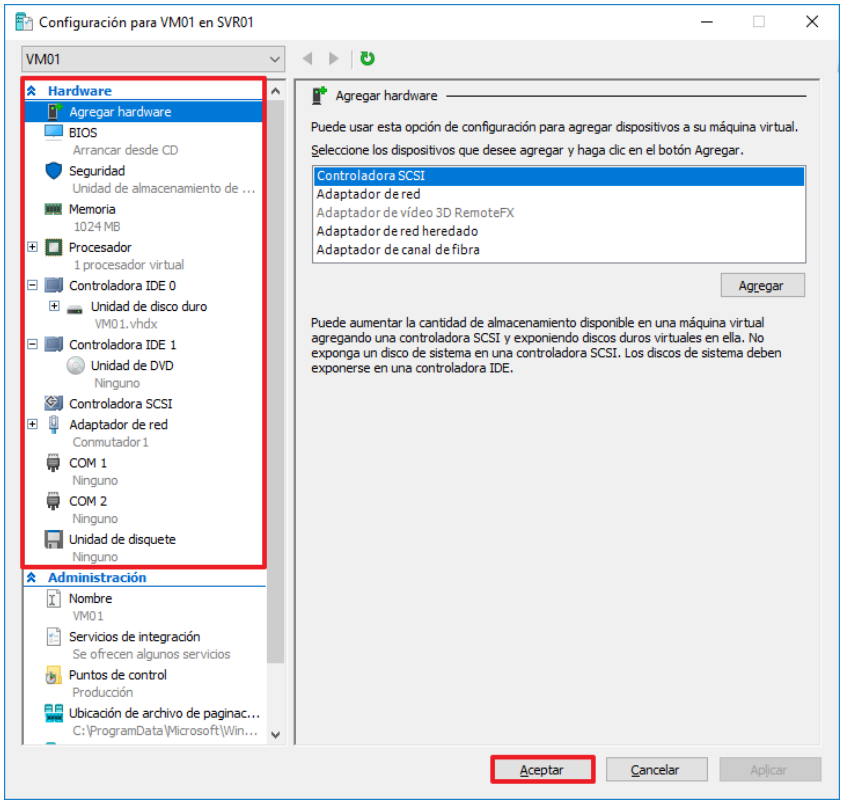
Paso	Descripción
72.	En la ventana “Especificar el nombre y la ubicación” determine el nombre que poseerá la máquina dentro de Hyper-V y una ubicación concreta si lo desea. Pulse “Siguiente >” para continuar.  **Nota:** Tenga en consideración que si realizó alguna modificación en el apartado “2.2 CONFIGURACIÓN GENERAL DE HYPER-V” la ubicación por defecto ya deberá estar configurada a la requerida por su organización. En este ejemplo se crea la máquina “VM01”, deberá adaptar los nombres a las necesidades de su organización”.
73.	En la ventana “Especificar generación” deberá determinar la generación de las máquinas creadas. Esto afectará en las características de las mismas. Pulse “Siguiente >” cuando haya finalizado.  **Nota:** En este ejemplo se opta por marcar “Generación 1”. Esta configuración deberá adaptarse a las necesidades de su organización. Una vez creada la máquina esta configuración no puede modificarse. Tenga este hecho presente de cara a futuras configuraciones que puedan ser requeridas como el “ANEXO A.5.2 CIFRADO DE MÁQUINAS VIRTUALES”.

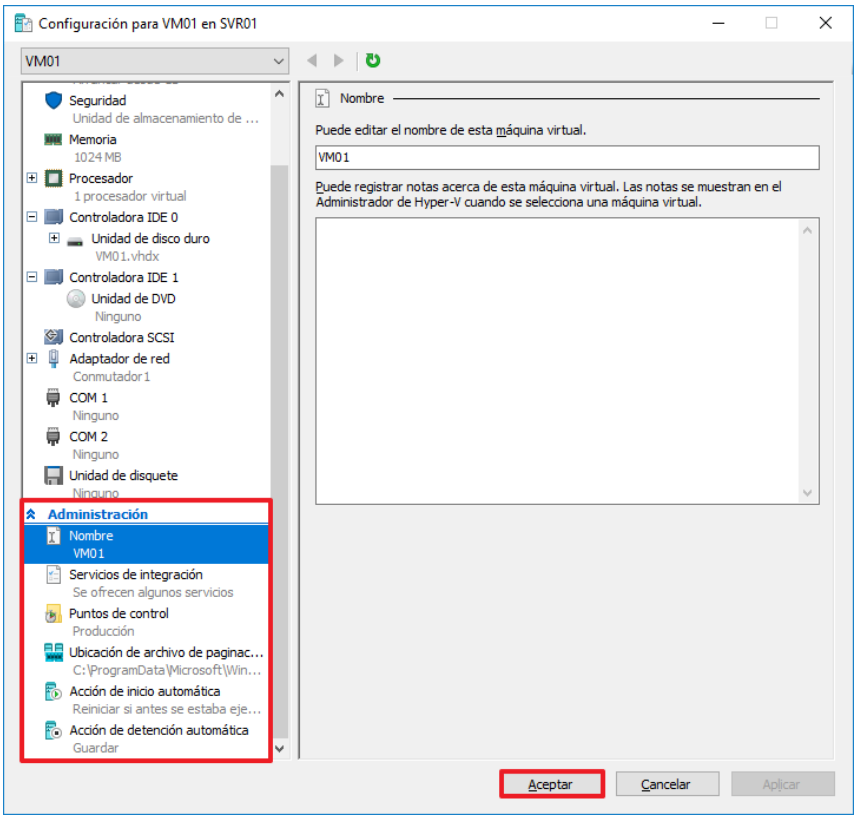
Paso	Descripción
74.	En la ventana “Asignar memoria” deberá determinar la memoria RAM de la máquina virtual. Además, podrá establecer el uso de memoria RAM de forma dinámica si lo desea. Pulse “Siguiente >” para seguir con el asistente.  **Nota:** Dependiendo de los recursos y las especificaciones de la máquina a implementar deberá configurar este valor. En este ejemplo se asigna “1024 MB” de memoria RAM.
75.	En la ventana “Configurar funciones de red” asigne uno de los conmutadores de los que disponga ya configurados. Pulse sobre el botón “Siguiente >” cuando finalice.  **Nota:** Deberá conectar el adaptador deseado en función de las necesidades de su organización. Esta configuración puede modificarse también tras crear la máquina. En este ejemplo se asigna el adaptador “Conmutador1”.

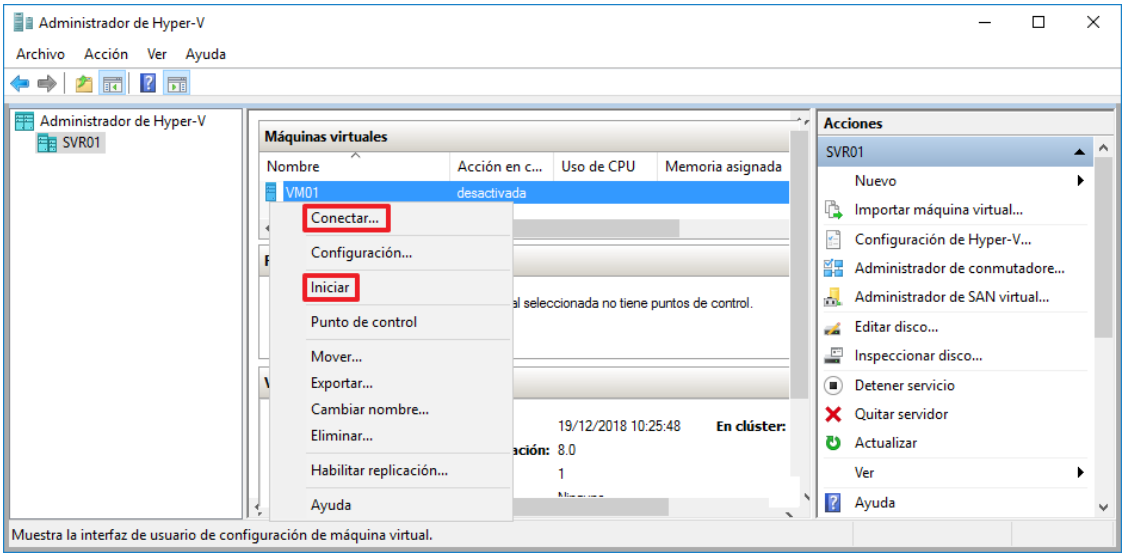
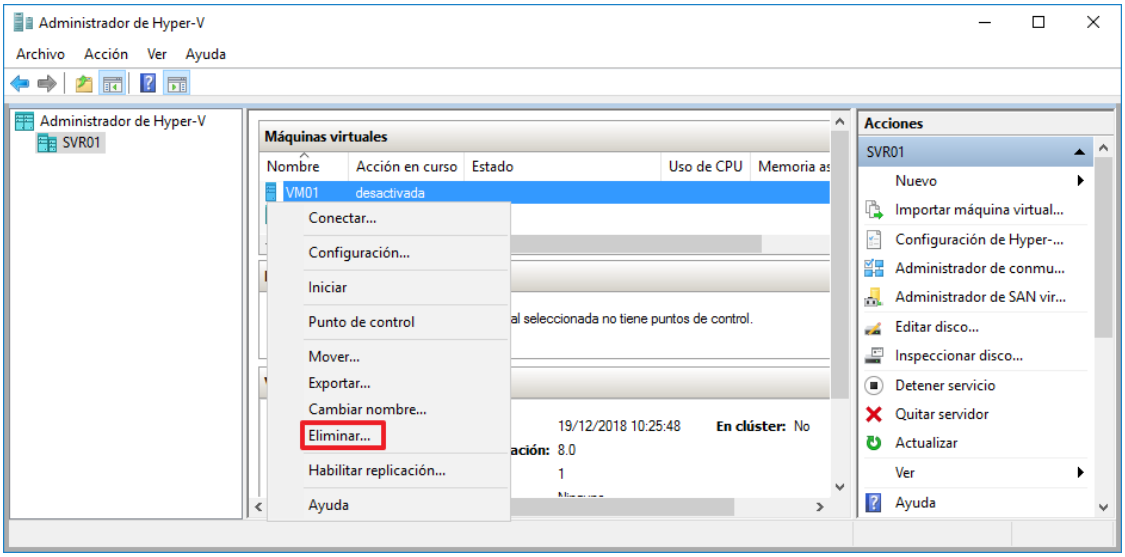
Paso	Descripción
76.	En la ventana “Conectar disco duro virtual” cree un disco duro virtual nuevo, asigne uno ya creado u omita este paso para exponer el disco más adelante. Pulse “Siguiente >” para continuar.  **Nota:** En este ejemplo se crea un disco virtual vacío con 50 GB de tamaño. Adapte el tamaño y la configuración a las necesidades de su organización.
77.	En la ventana “Opciones de instalación” configure un medio de arranque para la máquina virtual. Pulse “Siguiente >” cuando finalice.  **Nota:** En este ejemplo de opta por instalar un sistema operativo más adelante. Adapte este paso a las necesidades de su organización.

Paso	Descripción
78.	Por último, en la ventana “Resumen” compruebe que las configuraciones de la máquina virtual son correctas. En caso afirmativo pulse “Finalizar”. Si por el contrario requiere modificar alguna configuración pulse el botón “< Anterior” hasta llegar a la ventana deseada y modifique la configuración.
79.	Comenzará el proceso de creación el cual podrá variar dependiendo de las especificaciones de la máquina virtual. 
80.	Cuando haya finalizado la máquina virtual aparecerá en el panel central de “Administrador de Hyper-V”. 
81.	Para modificar la configuración establecida durante la creación o bien añadir más recursos haga clic derecho sobre la máquina deseada y pulse sobre la opción del menú contextual “Configuración…”. 

Paso	Descripción
82.	De mismo modo podrá realizar diferentes configuraciones que afectan al comportamiento de la máquina virtual y a la experiencia de usuario con dicha máquina. Pulse “Aceptar” cuando haya finalizado.

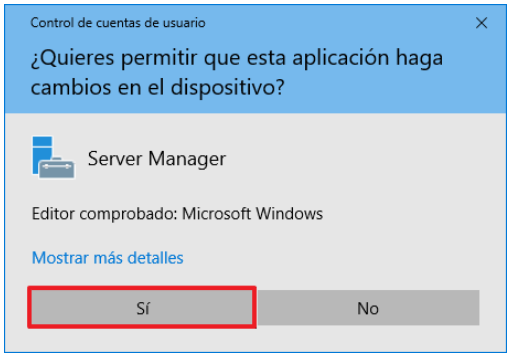


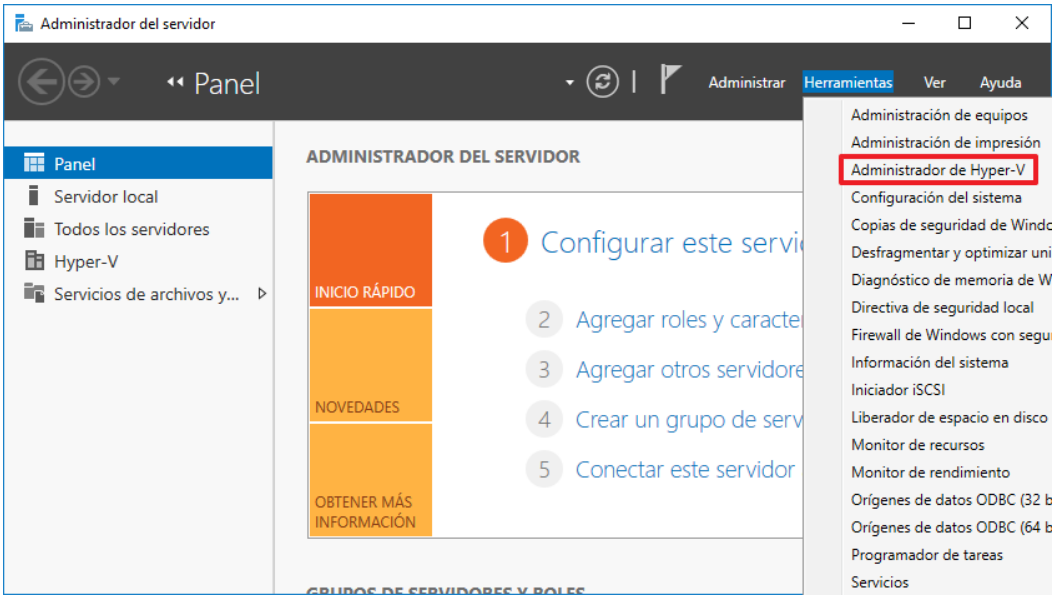
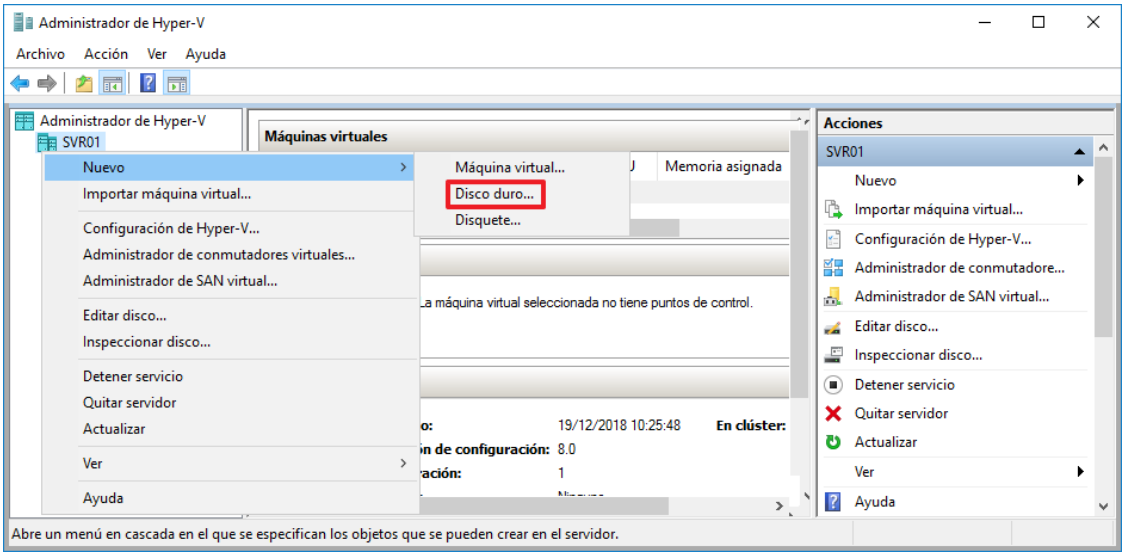


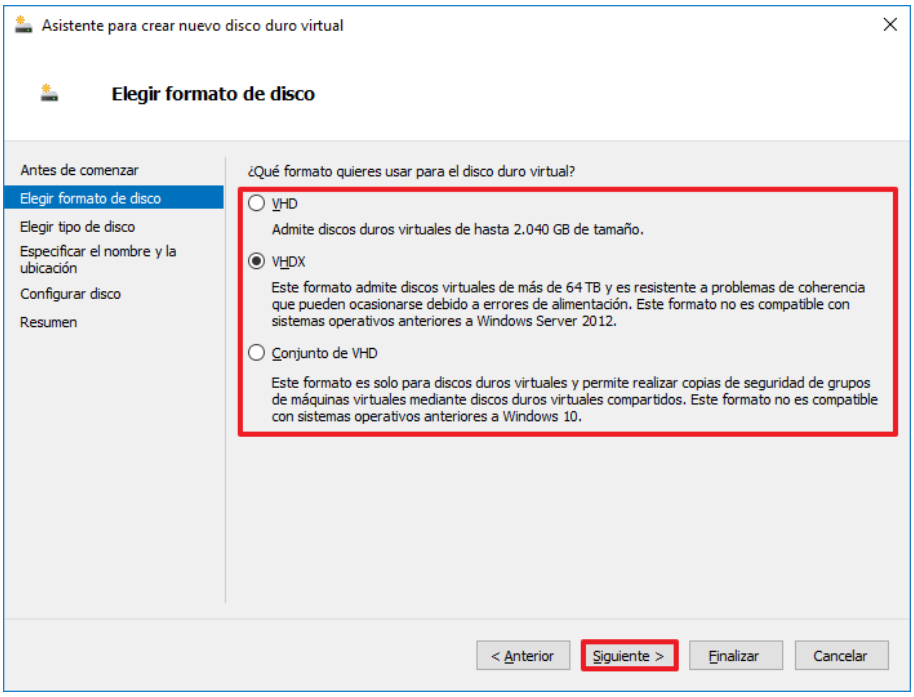
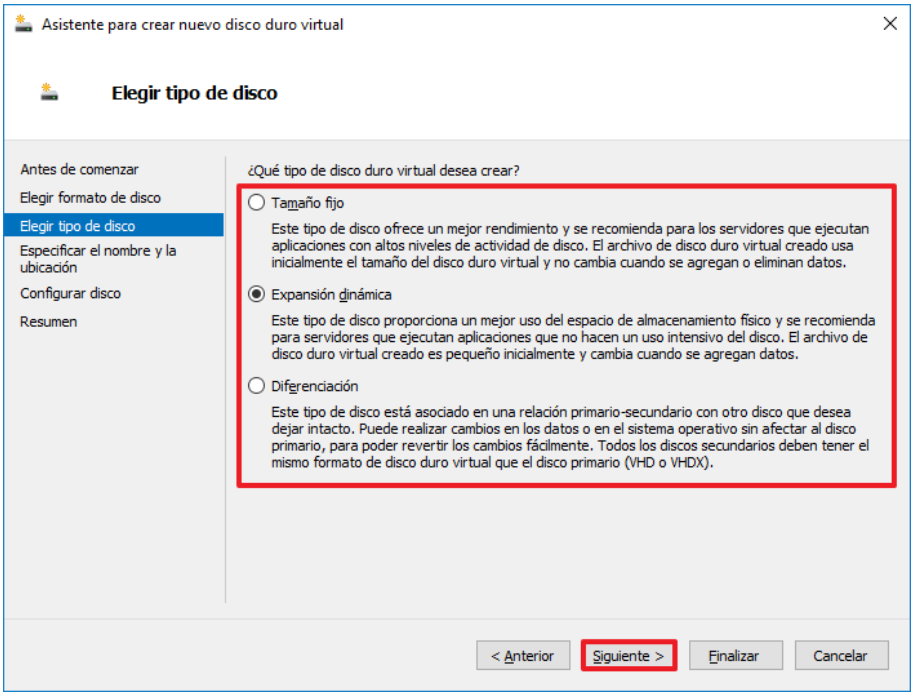
Paso	Descripción
83.	Por último, cuando la máquina esté finalizada podrá iniciarla y conectar con ella haciendo clic derecho y pulsando sobre las opciones del menú contextual “Iniciar” y “Conectar”, respectivamente. 
84.	En el caso de no disponer de disco virtual deberá consultar el apartado siguiente “2.5 GESTIÓN DE DISCOS DUROS VIRTUALES”.
85.	Si desea eliminar alguna de las máquinas haga clic derecho sobre ella y seleccione la opción del menú contextual “Eliminar…”.  **Nota:** Tenga en consideración que la eliminación de los discos asociados a la máquina deberá realizarse de forma manual.

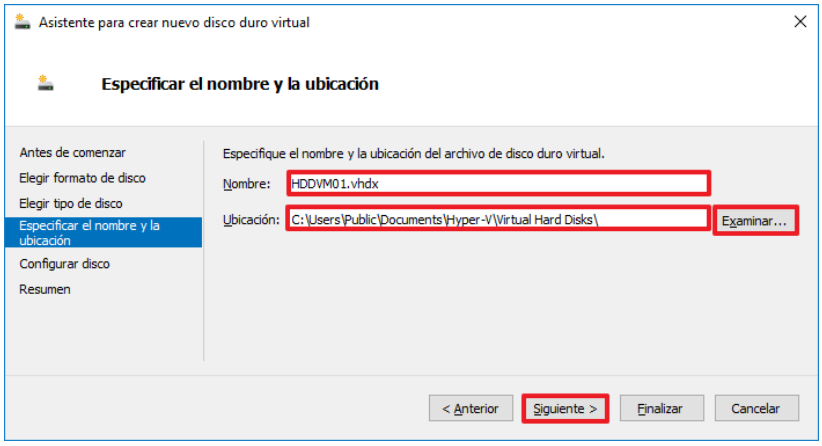
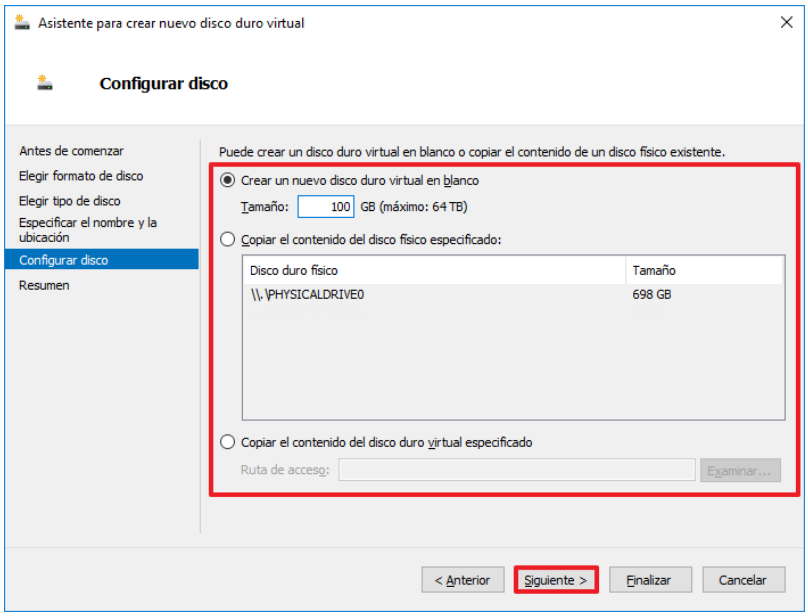
2.5. GESTIÓN DE DISCOS DUROS VIRTUALES

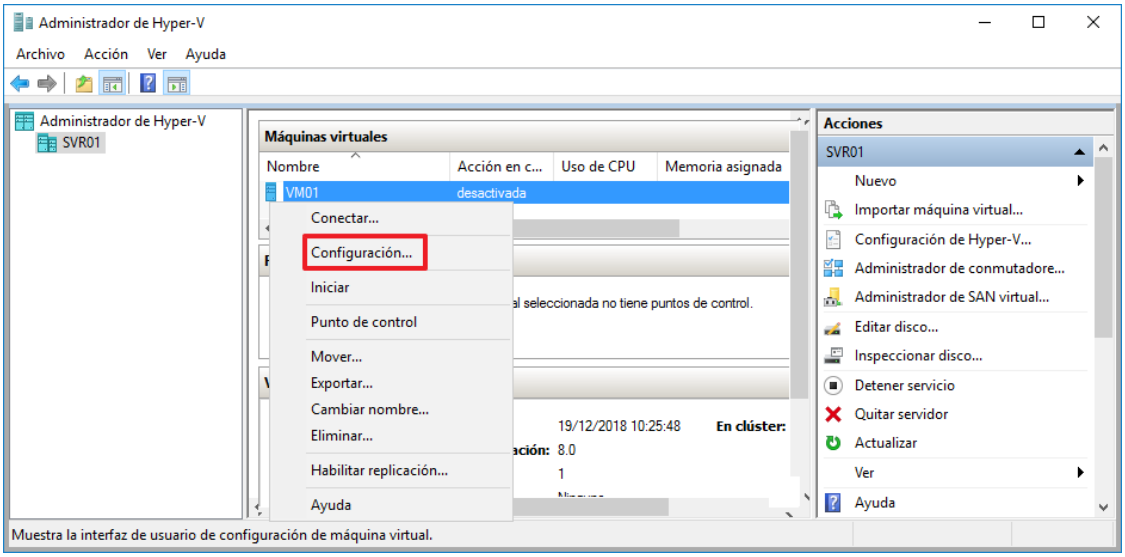
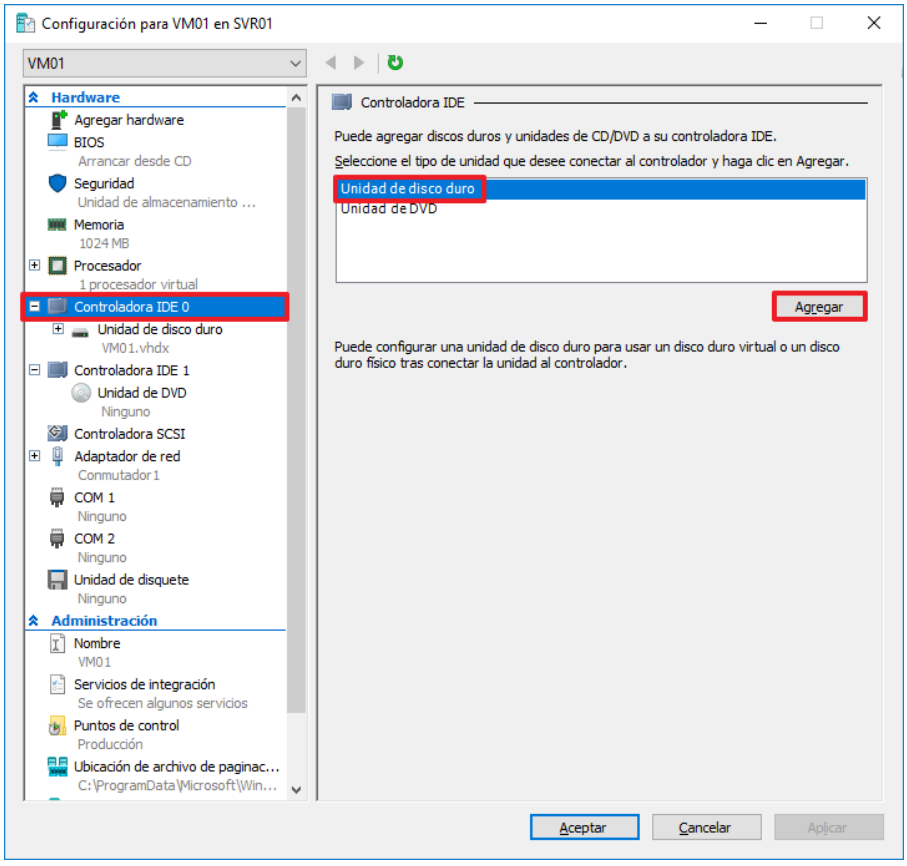
Los discos virtuales son el componente sobre el que sobre el que se apoyan las máquinas virtuales para almacenar los recursos que se generan al igual que sucede en un equipo real. Este apartado define un ejemplo para crear un disco virtual que pueda ser utilizado con diferentes fines, bien como disco principal de una máquina o como disco adicional.

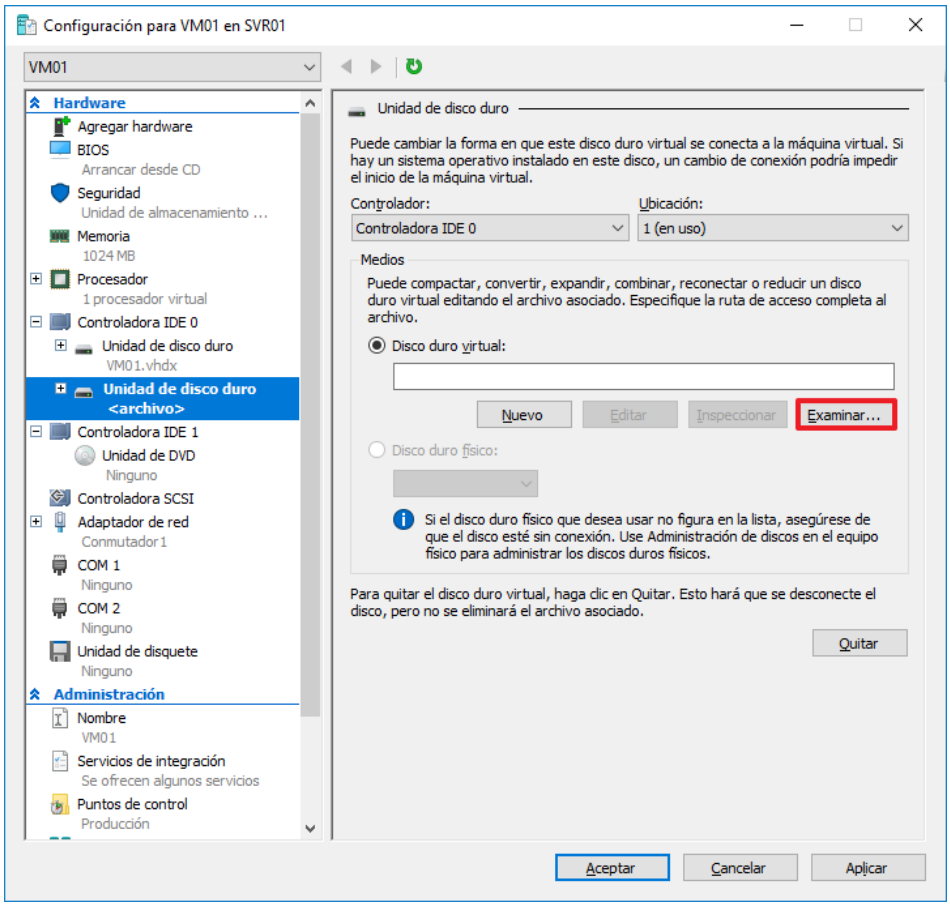
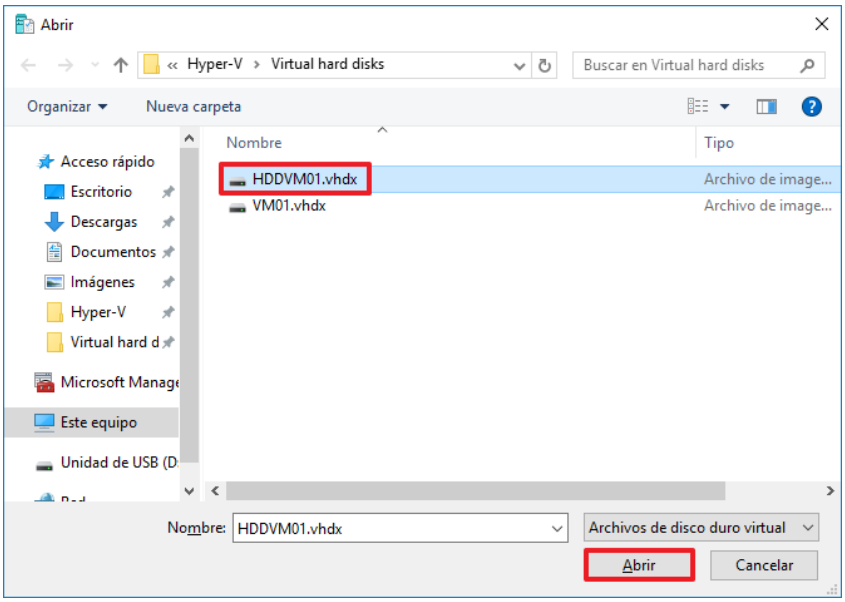
Paso	Descripción
86.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
87.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
88.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 

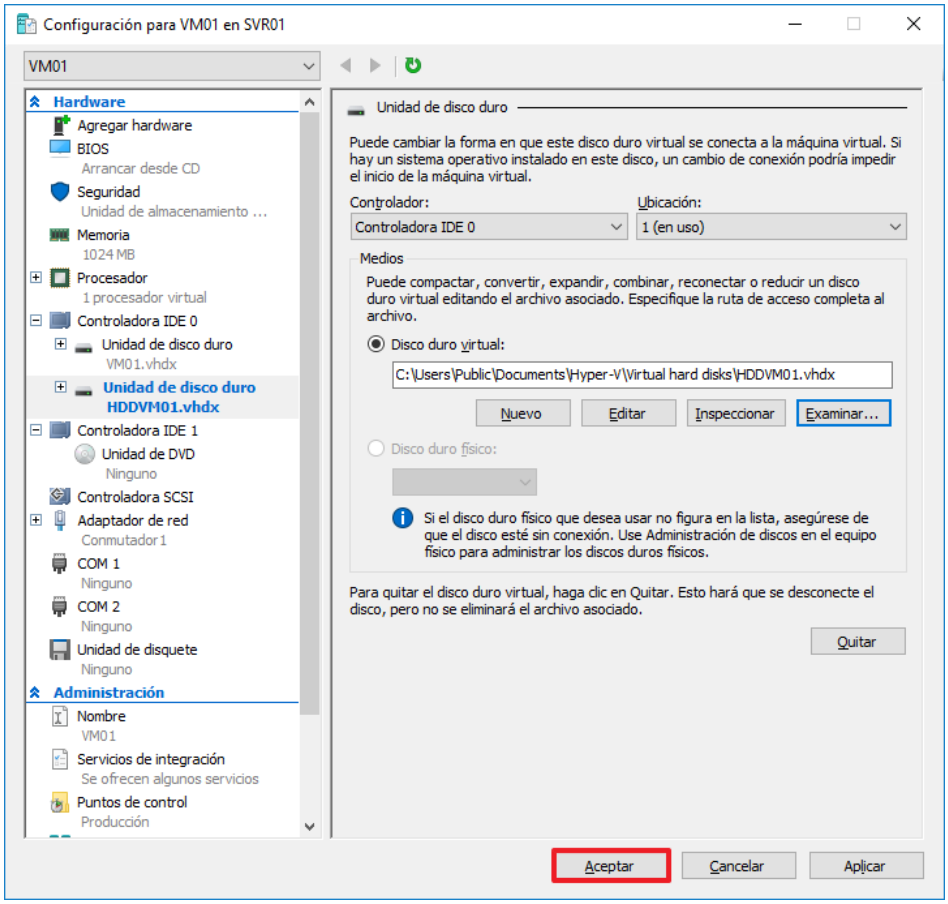
Paso	Descripción
89.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
90.	Dentro de la consola emergente seleccione el servidor de Hyper-V con el botón derecho y seleccione la opción del menú contextual **"Nuevo → Disco duro…"**.  **Nota:** En este ejemplo el servidor de denomina "SVR01". Deberá adaptar estos pasos a las configuraciones de su organización.
91.	Aparecerá el asistente para la creación de discos virtuales. En la ventana "Antes de comenzar" pulse "Siguiente >".

Paso	Descripción
92.	En la ventana “Elegir el formato de disco” deberá determinar el formato del disco dependiendo de las necesidades de su organización y de las máquinas virtuales que disponga. Pulse el botón “Siguiente >” para continuar.  **Nota:** En este ejemplo se crea un disco con formato “VHDX”.
93.	En la ventana “Elegir tipo de disco” deberá seleccionar como se dimensiona el disco cuando este almacena datos. Pulse “Siguiente >” cuando haya finalizado.  **Nota:** En este ejemplo se opta por una “Expansión dinámica” del disco.

Paso	Descripción
94.	En la ventana “Especificar el nombre y ubicación” determine el nombre asociado al disco virtual y donde va a ser almacenado. Pulse “Siguiente >” para continuar.  **Nota:** Tenga en consideración que si realizó alguna modificación en el apartado “2.2 CONFIGURACIÓN GENERAL DE HYPER-V” la ubicación por defecto ya deberá estar configurada a la requerida por su organización. En este ejemplo se asigna el nombre “HDDVM01”.
95.	En la ventana “Configurar disco” deberá determinar las necesidades del disco duro creado pudiendo crear un disco en blanco (sin datos) o con datos copiados de otro disco existente. Pulse “Siguiente >” para continuar con el asistente.  **Nota:** En este ejemplo se genera un disco de 100 GB en blanco para asociarlo a una máquina virtual existente.
96.	Por último, en la ventana “Resumen” compruebe que las configuraciones del disco son correctas. En caso afirmativo pulse “Finalizar”. Si por el contrario requiere modificar alguna configuración pulse el botón “< Anterior” hasta llegar a la ventana deseada y modifique la configuración.

Paso	Descripción
97.	Para asignar el disco recién creado seleccione la máquina afectada con el botón derecho y pulse sobre la opción del menú contextual “Configuración…”.  **Nota:** En este ejemplo se hace uso de la máquina virtual “VM01”. Adapte este y los siguientes pasos a las necesidades de su organización. La máquina virtual deberá estar apagada para realizar los siguientes pasos.
98.	Sitúese sobre el apartado “Controladora IDE 0” y en el panel derecho seleccione “Unidad de disco duro”. Pulse sobre “Agregar” para continuar. 

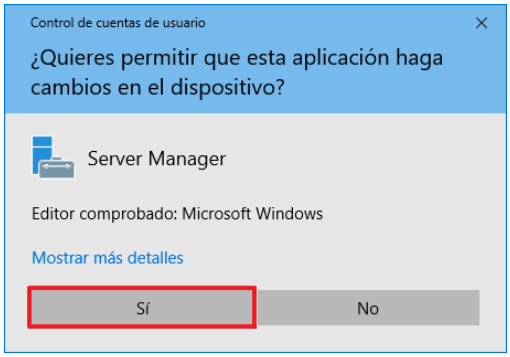
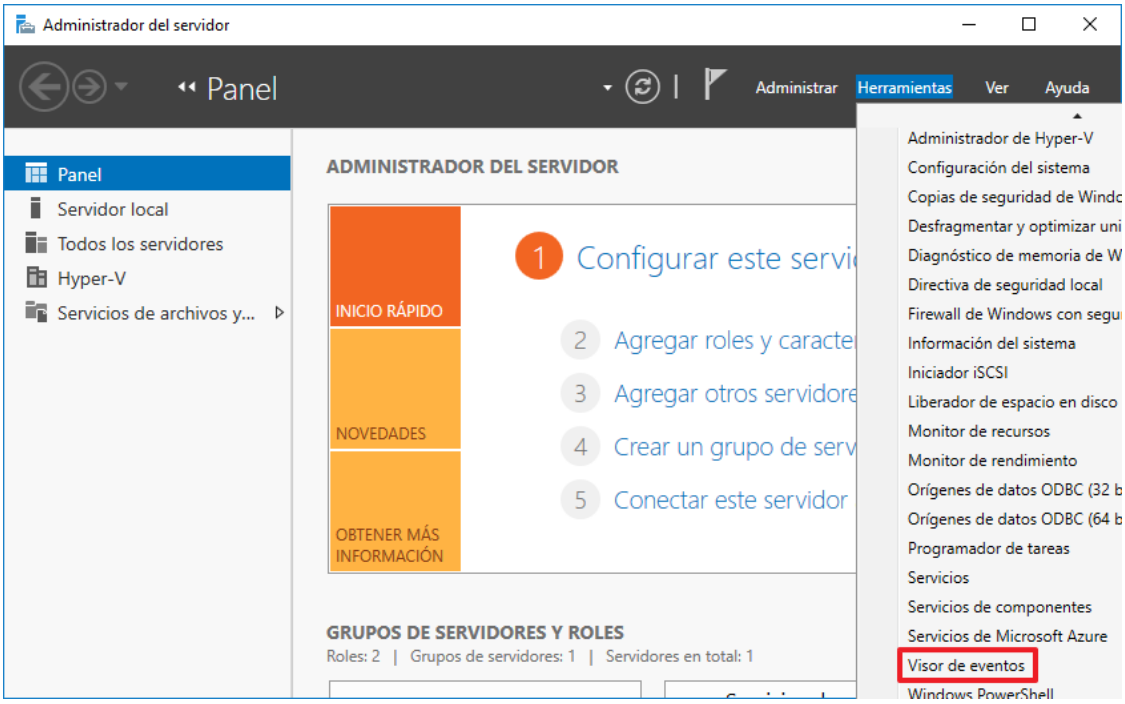
Paso	Descripción
99.	De nuevo en el panel derecho seleccione el botón “Examinar”. 
100.	Ubíquese sobre la ruta en la que se creó el disco duro virtual, selecciónelo y pulse el botón “Abrir”. 

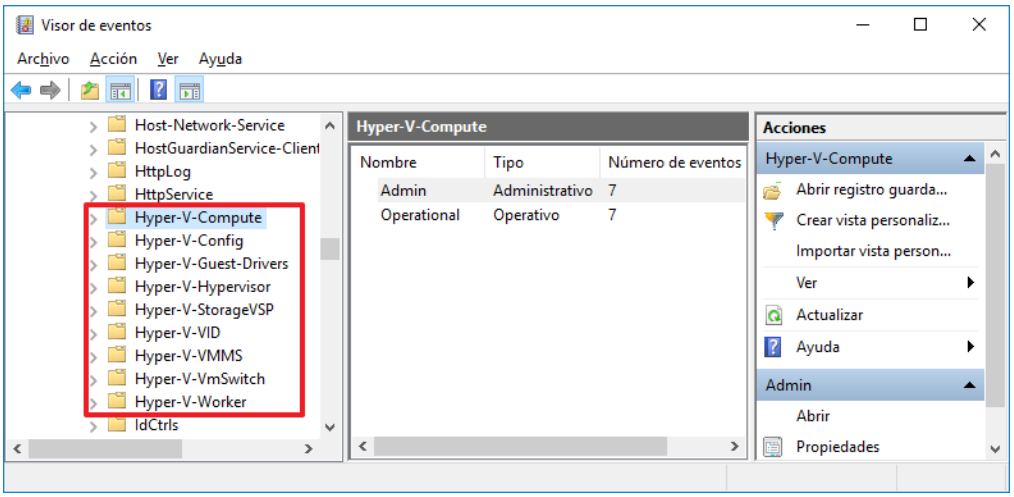
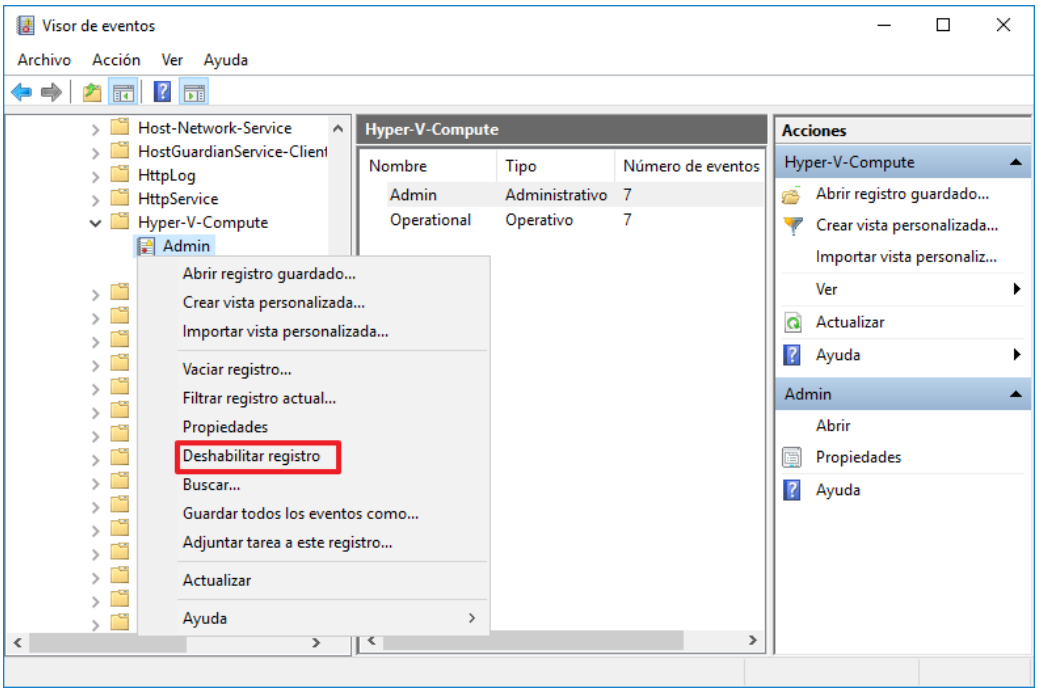
Paso	Descripción
101.	Por último, pulse “Aceptar” para guardar los cambios. A partir de este momento la máquina virtual estará en posesión de un disco duro adicional. 

2.6. REGISTRO DE EVENTOS EN HYPER-V

Todos los eventos que se suceden en el servidor de Hyper-V deben ser recogidos por el equipo con el fin de determinar las acciones realizadas sobre el propio servidor y sobre las máquinas que este alberga.

Paso	Descripción
102.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

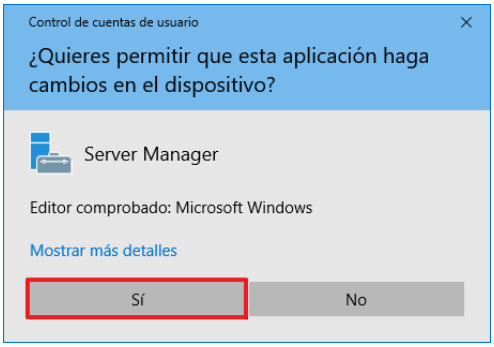
Paso	Descripción
103.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
104.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
105.	Inicie la herramienta "Visor de eventos". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Visor de eventos"**. 

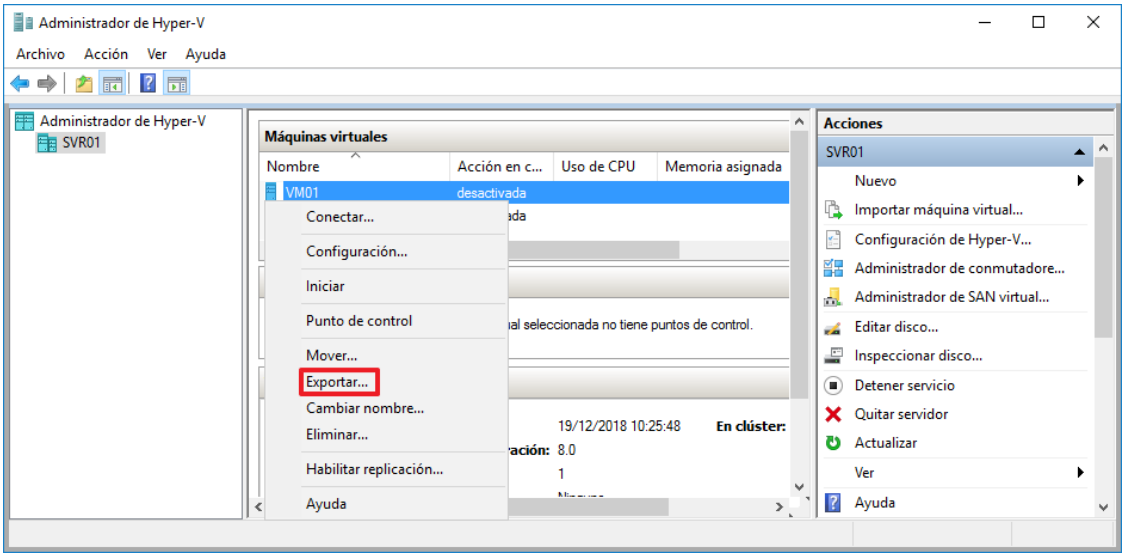
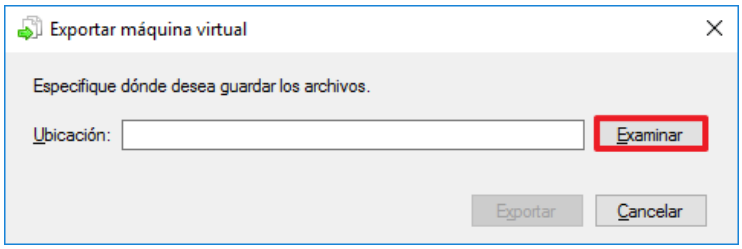
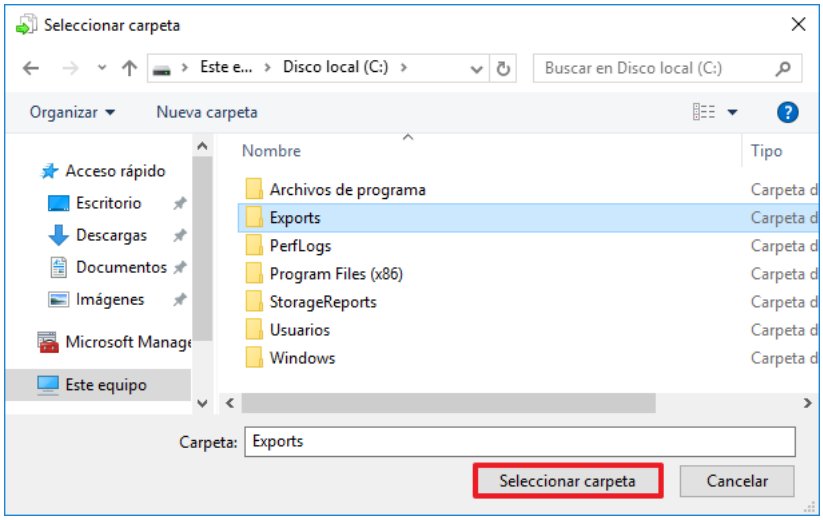
Paso	Descripción
106.	En consola "Visor de eventos" despliegue el nodo **"Visor de eventos (local) → Registro de aplicaciones y servicios → Microsoft → Windows"**. En el listado de carpetas sitúese sobre aquellas que hagan referencia a Hyper-V.  **Nota:** Puede obtener más información acerca de los eventos registrados por Hyper-V en el siguiente enlace: https://blogs.technet.microsoft.com/virtualization/2018/01/23/looking-at-the-hyper-v-event-log-january-2018-edition/
107.	Por último, asegúrese que dentro de cada directorio se encuentra activado el registro haciendo clic derecho sobre cada uno de los elementos. En el caso de que el registro este habilitado aparecerá la opción "Deshabilitar registro". Si por el contrario no se encuentra habilitado el registro aparecerá la opción "Habilitar registro. 

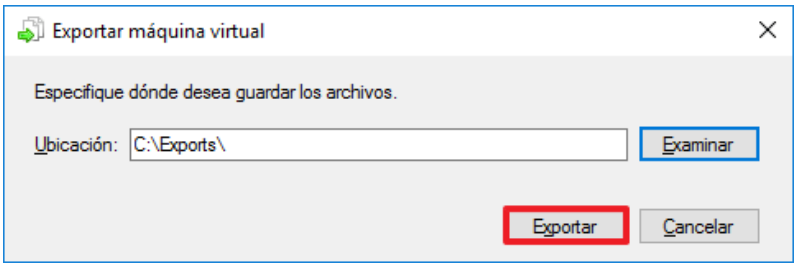
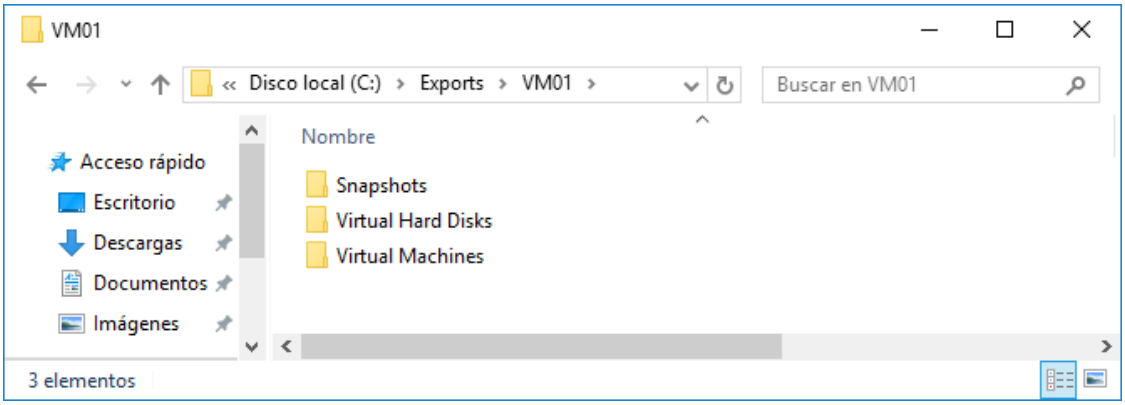
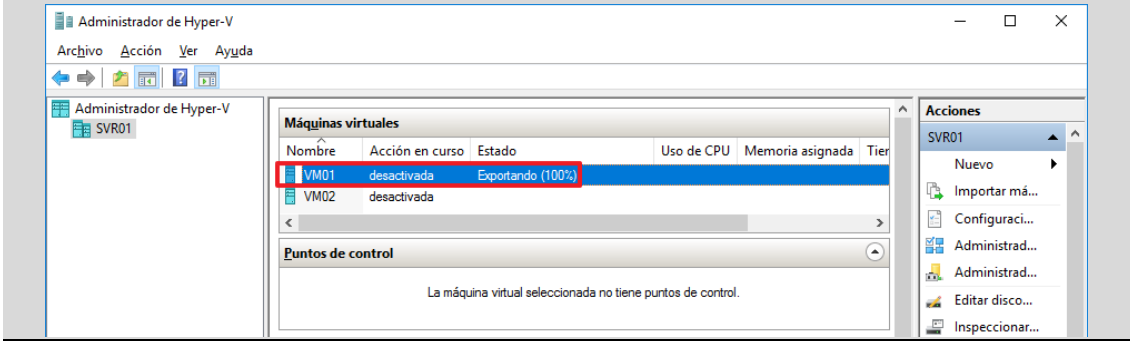
2.7. COPIAS DE SEGURIDAD DE MÁQUINAS VIRTUALES

Hyper-V dispone de varias opciones para realizar copias de seguridad de las máquinas con el objetivo de mantener la continuidad y evitar la pérdida de datos. Aunque tal y como se explicó en apartados anteriores es posible configurar un servidor como equipo de réplicas se va a optar por una opción que permite realizar copias si no se dispone de un servidor adicional.

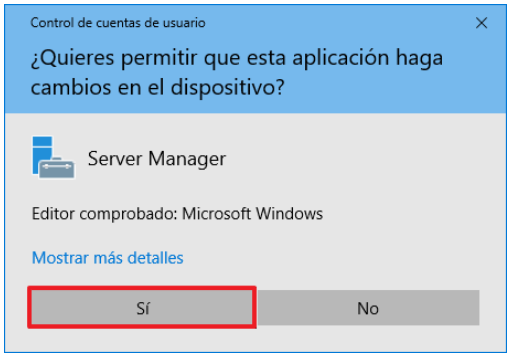
2.7.1. EXPORTAR MÁQUINAS VIRTUALES

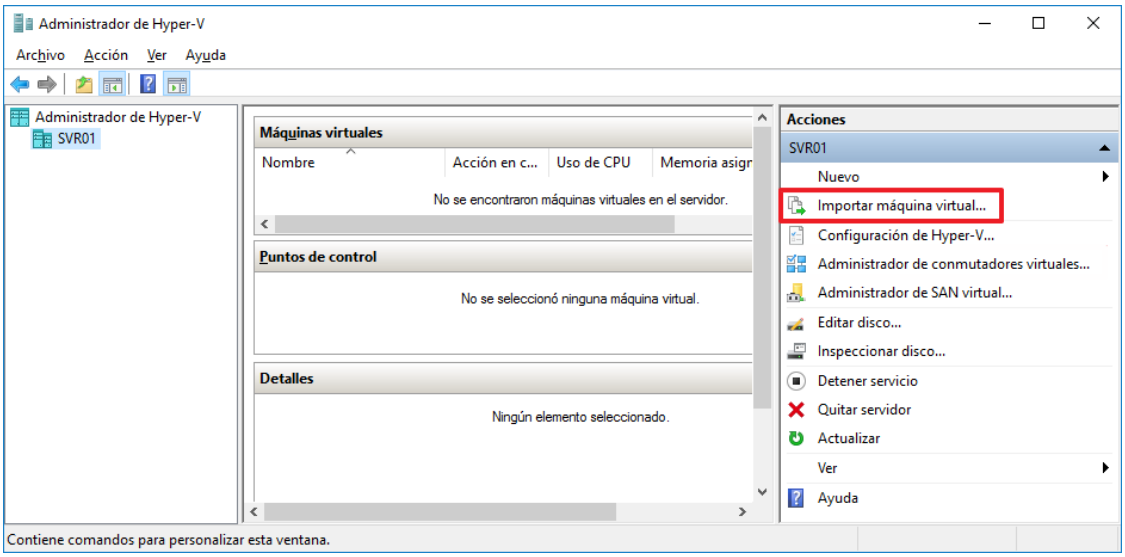
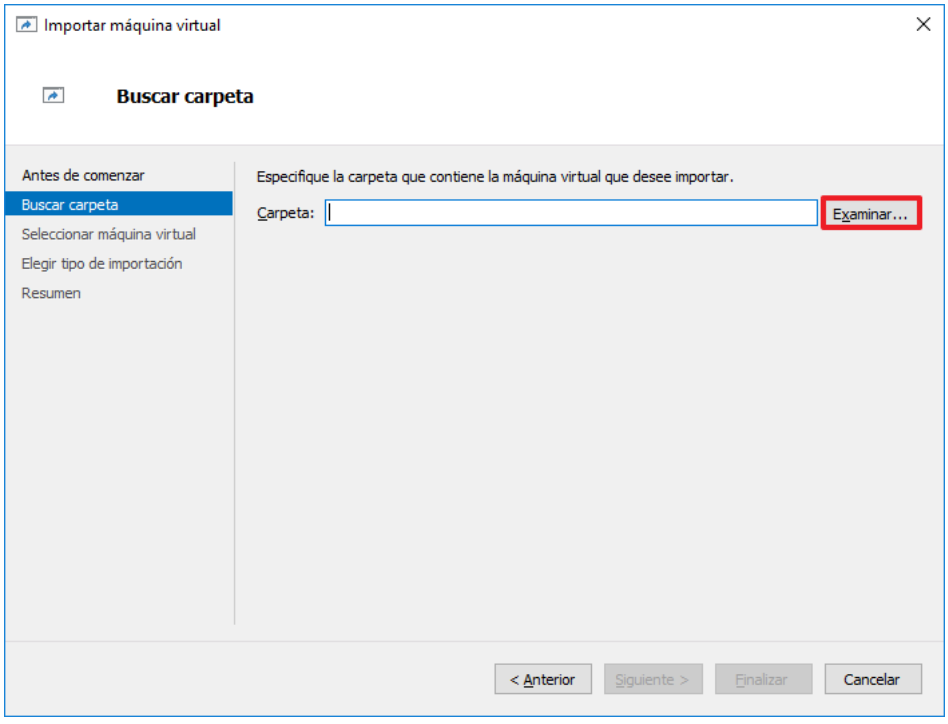
Paso	Descripción
108.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
109.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas.
110.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
111.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 

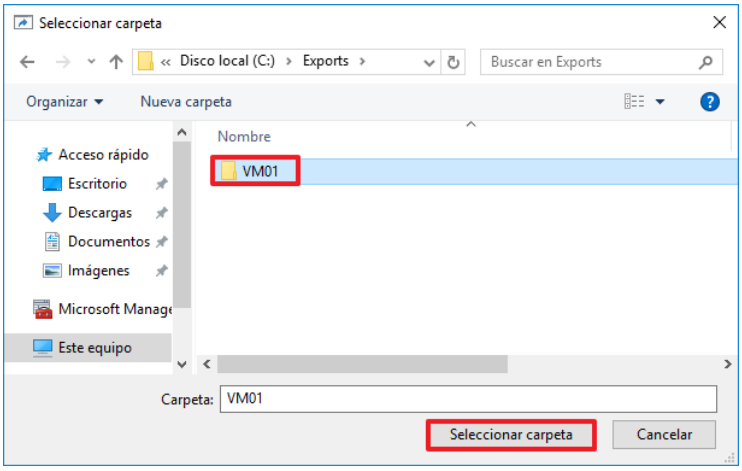
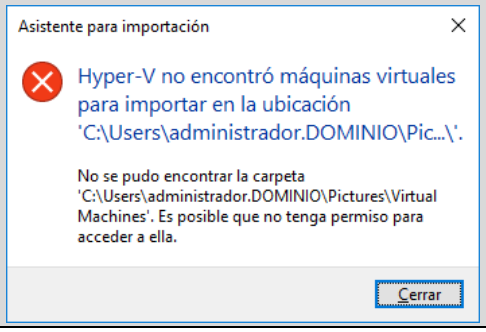
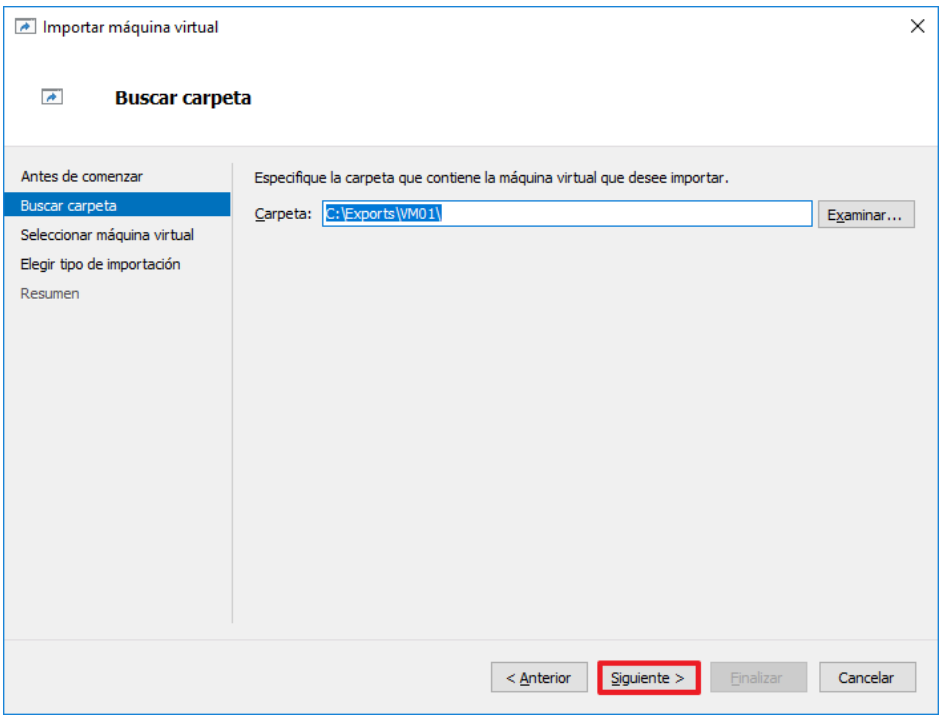
Paso	Descripción
112.	Seleccione la máquina virtual sobre la que desea realizar una copia de seguridad y pulse sobre la opción “Exportar…”.  **Nota:** En este ejemplo se realiza la exportación de la máquina “VM01”.
113.	En la ventana emergente pulse sobre el botón “Examinar”. 
114.	Seleccione la ubicación sobre la que desea exportar la máquina y pulse sobre el botón “Seleccionar carpeta”.  **Nota:** En este ejemplo se utiliza el directorio “Exports” ubicado en “C:\”.

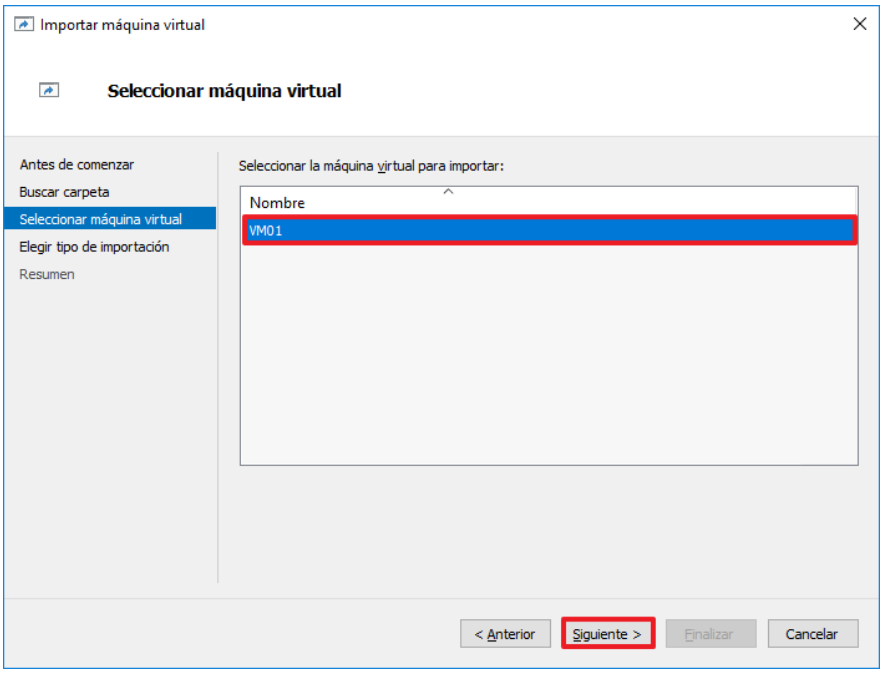
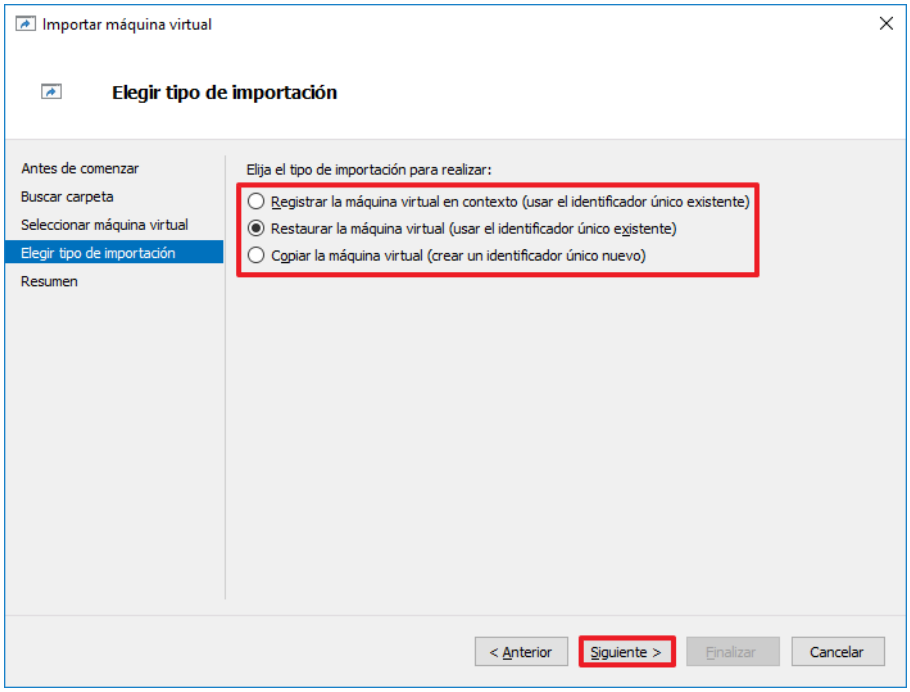
Paso	Descripción
115.	Pulse sobre el botón “Exportar” para comenzar con la copia. 
116.	Cuando el proceso haya finalizado la consola de Hyper-V lo notificará en el apartado correspondiente al “Estado” y dentro del directorio seleccionado se habrá generado un directorio con todos los componentes de la máquina virtual.  **Nota:** Dependiendo del tamaño de la máquina el tiempo podrá variar. La consola de Hyper-V mostrará en todo caso el porcentaje de estado. 

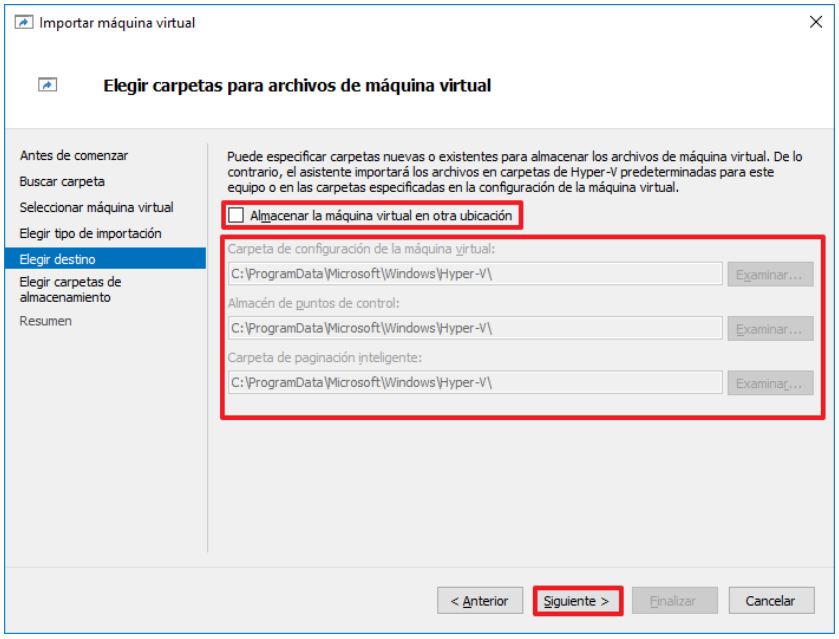
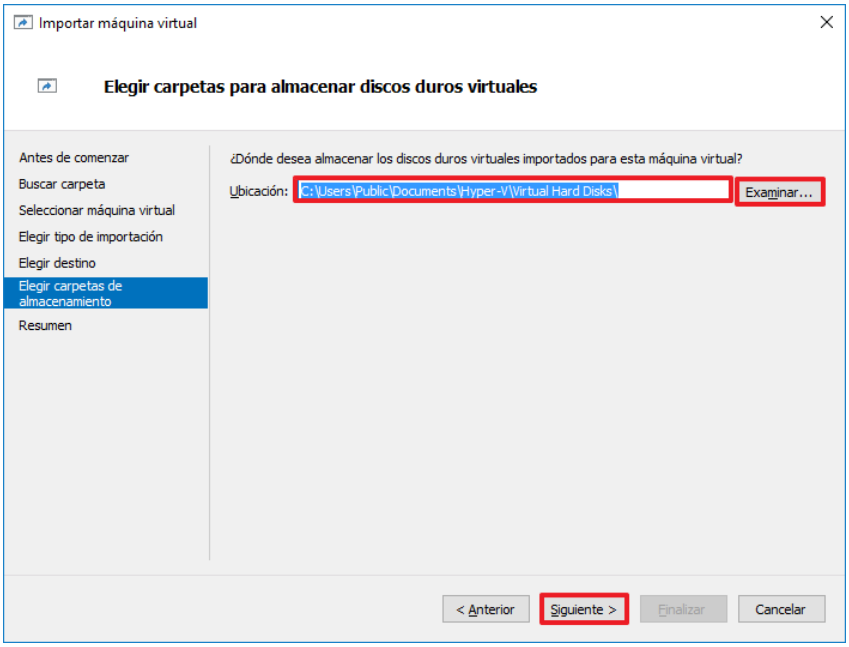
2.7.2. IMPORTAR MÁQUINAS VIRTUALES

Paso	Descripción
117.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
118.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
119.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
120.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 

Paso	Descripción
121.	Seleccione la opción del panel derecho “Importar máquina virtual…”. 
122.	Se iniciará el asistente para importar una máquina virtual. Pulse “Siguiente >” en la ventana “Antes de comenzar”.
123.	En la ventana “Buscar carpeta” pulse sobre el botón “Examinar…”. 

Paso	Descripción
124.	A continuación, seleccione el directorio donde se encuentre la máquina virtual y pulse sobre “Seleccionar carpeta”.  **Nota:** Si selecciona una ubicación incorrecta el asistente notificará un error. 
125.	Pulse el botón “Siguiente >” para continuar con la importación. 

Paso	Descripción
126.	Seleccione la máquina virtual que desea importar y pulse “Siguiente >”.  **Nota:** Es posible que la ruta indicada posea varias máquinas virtuales para importar, por lo que deberá seleccionar aquella que corresponda.
127.	En la ventana elegir tipo de importación seleccione la opción más adecuado dependiendo de la operación a realizar con la máquina. Pulse “Siguiente >” para finalizar con la importación”.  **Nota:** En este ejemplo se hace uso de la opción “Restaurar la máquina virtual”. Dependiendo de la opción seleccionada deberá ejecutar más o menos pasos en el asistente.

Paso	Descripción
128.	En la ventana “Elegir destino” deberá establecer si lo desea una ruta para cada una de las configuraciones de la máquina virtual. Pulse “Siguiente >” cuando haya finalizado.  **Nota:** En este ejemplo se opta por ubicar los archivos en las rutas por defecto definidas en apartados anteriores.
129.	Al igual que sucedía en el paso anterior deberá ahora establecer la ubicación para los discos de la máquina virtual. Si no indica dicha ubicación se almacenarán en la ubicación predefinida en apartados anteriores. Pulse “Siguiente >” para continuar. 
130.	Por último, en la ventana “Resumen” compruebe que las configuraciones de la máquina virtual son correctas. En caso afirmativo pulse “Finalizar”. Si por el contrario requiere modificar alguna configuración pulse el botón “< Anterior” hasta llegar a la ventana deseada y modifique la configuración.

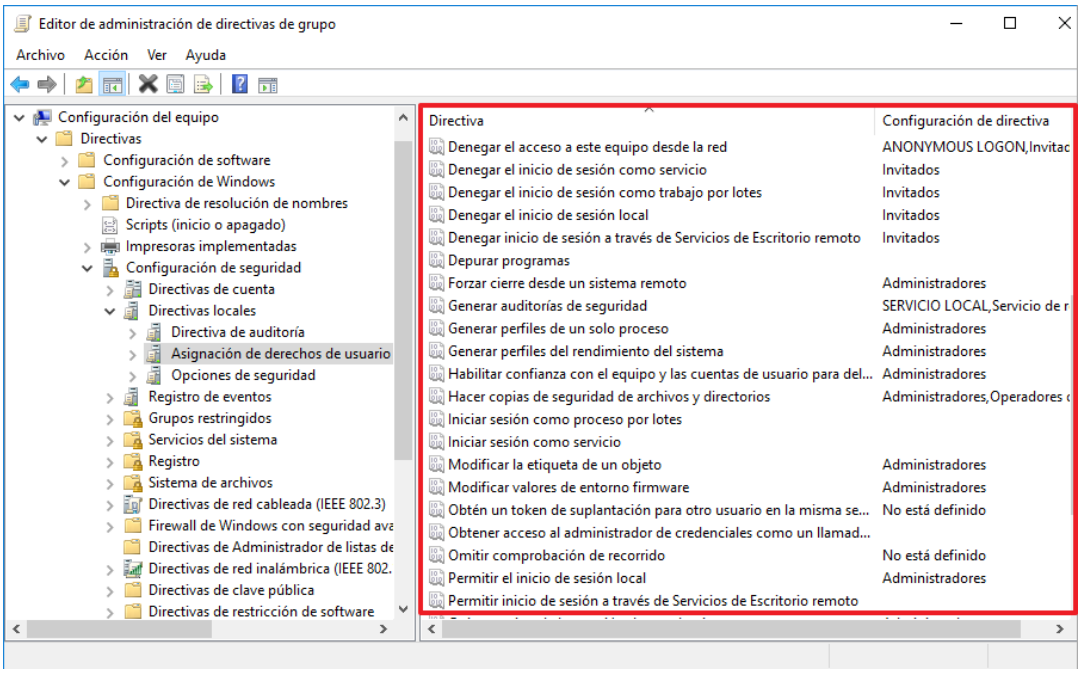
2.8. DERECHOS DE ACCESO SOBRE SISTEMAS OPERATIVOS MS WINDOWS VIRTUALIZADOS

Los permisos de acceso sobre los sistemas operativos MS Windows virtualizados dentro del servicio de Hyper-V debe quedar limitado a los usuarios legitimados para ello. Por lo tanto, será necesario establecer los permisos necesarios para limitar dicho acceso.

Deberá tener en consideración la asignación de permisos diferenciando si la conexión se realiza a un servidor o un equipo cliente. Deberá por tanto generar un objeto GPO incremental o modificar la configuración establecida con el fin de permitir o denegar el inicio de sesión sobre las máquinas virtuales.

En el presente apartado se trata el ejemplo de configurar dicha asignación de permisos a través del objeto GPO que configura el servidor de virtualización Hyper-V.

Paso	Descripción
131.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
132.	Ejecute el “Administrador del Servidor” desde el icono correspondiente.
133.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.
134.	A continuación, inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor”, abierta en pasos anteriores, seleccione **“Herramientas → Administración de directivas de grupo”.** 

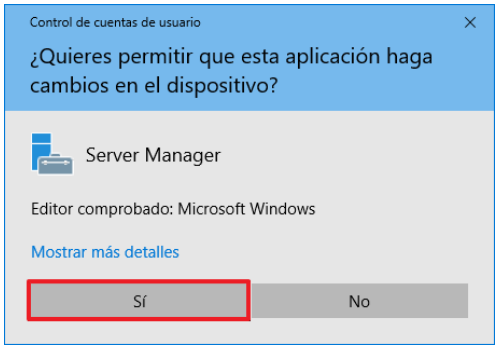
Paso	Descripción
135.	Los objetos de políticas de grupo para Controladores de Dominio y Servidores miembros especifican unos derechos de usuario siguiendo planteamientos de seguridad que aplican los principios de mínimo privilegio y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les hayan asignado derechos determinados para la administración o gestión de los sistemas. Si esto fuera así, deberá realizar las modificaciones pertinentes sobre el objeto de política de grupo que aplique sobre el sistema operativo virtualizado o bien editando la configuración de política de grupo local en el caso de un equipo no perteneciente a un dominio.
136.	Sobre el objeto de GPO que se quiere modificar, deberá pulsar clic derecho y seleccionar “Editar” en el menú desplegado.
137.	Una vez abierto el “Editor de administración de directivas de grupo”, despliegue la política y sitúese en la siguiente ruta. **“Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”** 
138.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales de acceso al sistema.
139.	Guarde la configuración cerrando la ventana de editor de administración de directivas de grupo.

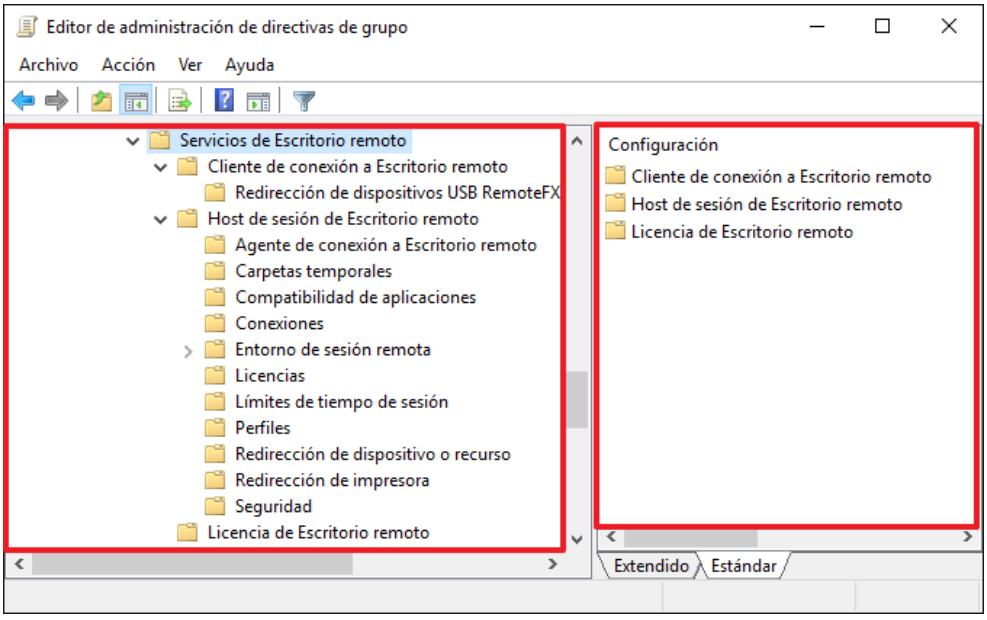
2.9. ACCESO REMOTO SOBRE SISTEMAS OPERATIVOS MS WINDOWS VIRTUALIZADOS

Del mismo modo que en el punto anterior, no basta con conceder permisos sobre los equipos cliente o servidores ubicados dentro del servidor de Hyper-V sino que además será necesario establecer los mecanismos seguros para las conexiones remotas a las máquinas virtuales que almacena Hyper-V.

En el presente apartado se definen las medidas a tomar en el caso de realizar una conexión remota a través del servicio Escritorio Remoto de Windows. Para definir dicha configuración deberá hacer uso de un objeto GPO incremental que configure la seguridad de dicho servicio o editar la configuración de un objeto GPO ya aplicado.

Para el presente ejemplo se realiza un ejemplo de configuración para escritorio remoto que asegure la conexión de este servicio al servidor de Hyper-V.

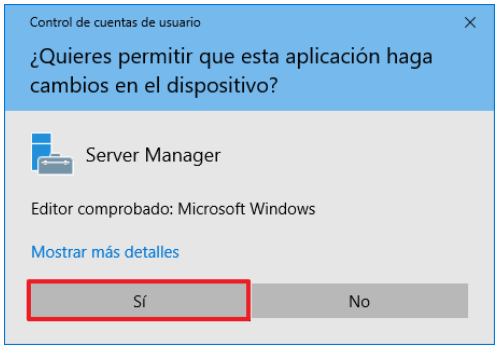
Paso	Descripción
140.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
141.	Ejecute el “Administrador del Servidor” desde el icono correspondiente. 
142.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 

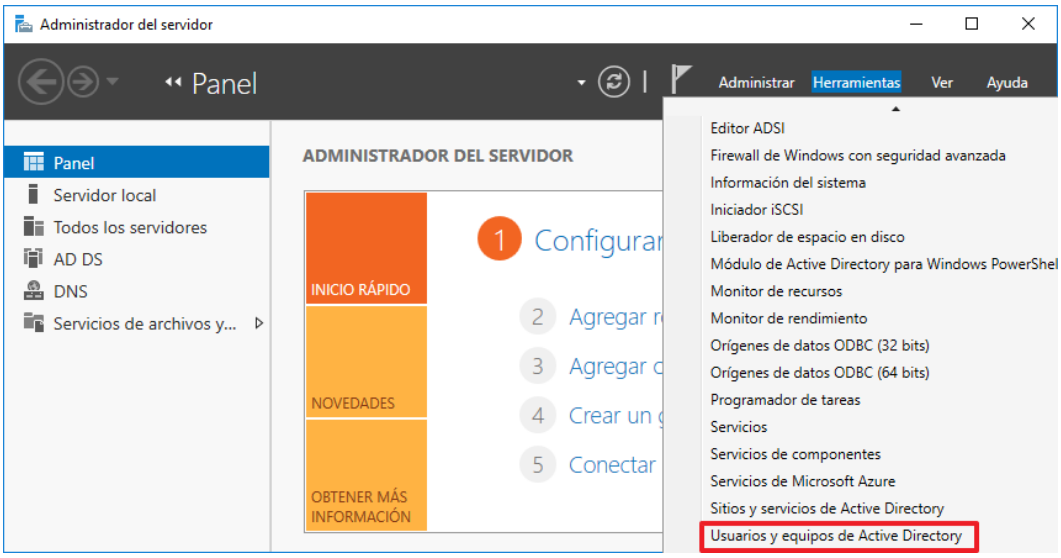
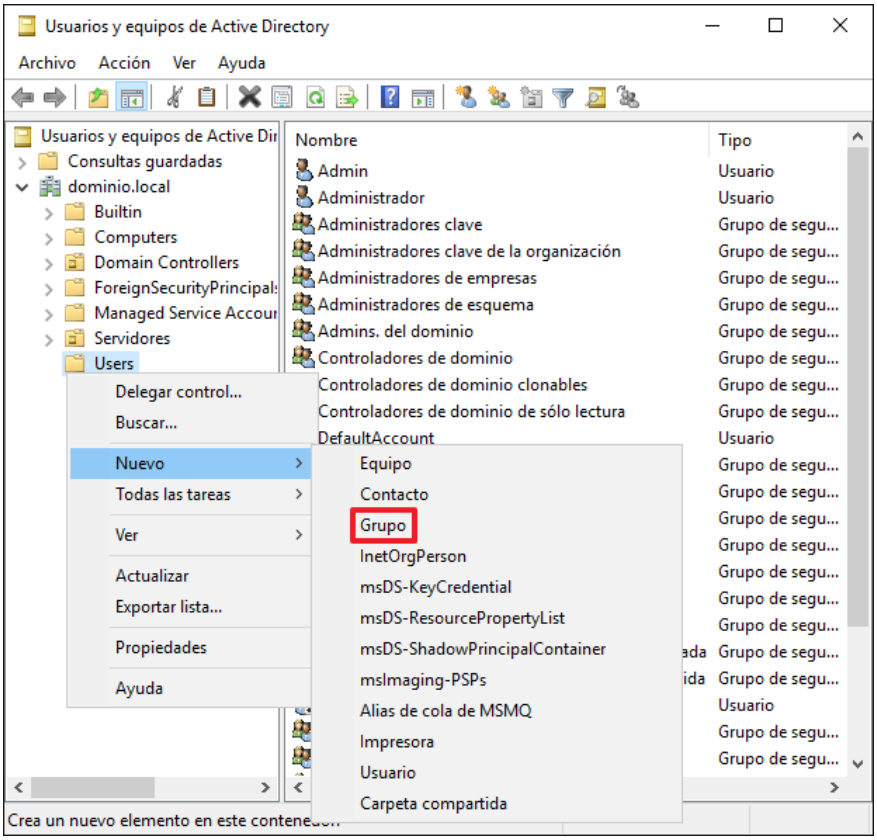
Paso	Descripción
143.	A continuación, inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor”, abierta en pasos anteriores, seleccione **“Herramientas → Administración de directivas de grupo”.** 
144.	Los elementos de plantillas administrativas permiten establecer la configuración segura a realizar sobre una conexión basada en servicios de escritorio remoto. Esta configuración permite que las conexiones realizadas a servidores y equipos cliente asegure la integridad de la conexión. Para establecer dicha configuración, deberá realizar las modificaciones pertinentes sobre el objeto de política de grupo que aplique sobre el sistema operativo virtualizado o bien editando la configuración de política de grupo local en el caso de un equipo no perteneciente a un dominio.
145.	Sobre el objeto de GPO que se quiere modificar, deberá pulsar clic derecho y seleccionar “Editar” en el menú desplegado.
146.	Una vez abierto el “Editor de administración de directivas de grupo”, despliegue la política y sitúese en la siguiente ruta. **“Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Servicios de Escritorio remoto”** 
147.	Modifique las directivas, estableciendo una configuración segura para el acceso remoto tanto a servidores como equipos cliente.
148.	Guarde la configuración cerrando la ventana de editor de administración de directivas de grupo.

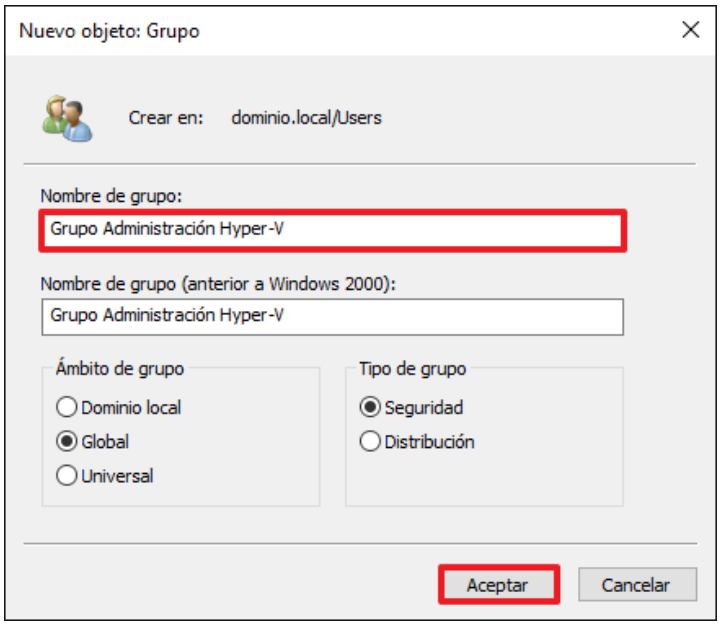
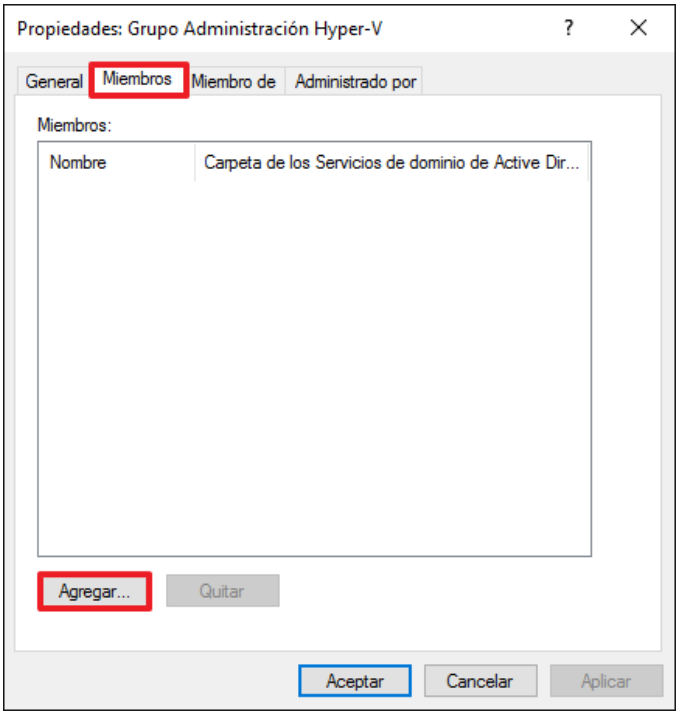
Paso	Descripción
149.	Adicionalmente a esta configuración deberá establecer los parámetros de red que permitan realizar la comunicación en red. Para ello haga uso de nuevo del objeto GPO correspondiente y configure el firewall para que permita la conexión entre equipos y los medios de autenticación correspondientes.
150.	Como última medida, y que es aplicable a partir la categoría media del ENS, deberá establecer las acciones permitidas y acciones no permitidas por la política de la organización durante el acceso remoto a las máquinas virtuales.

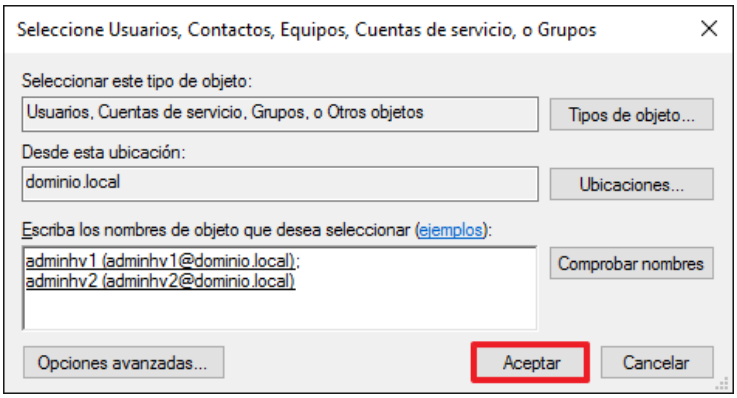
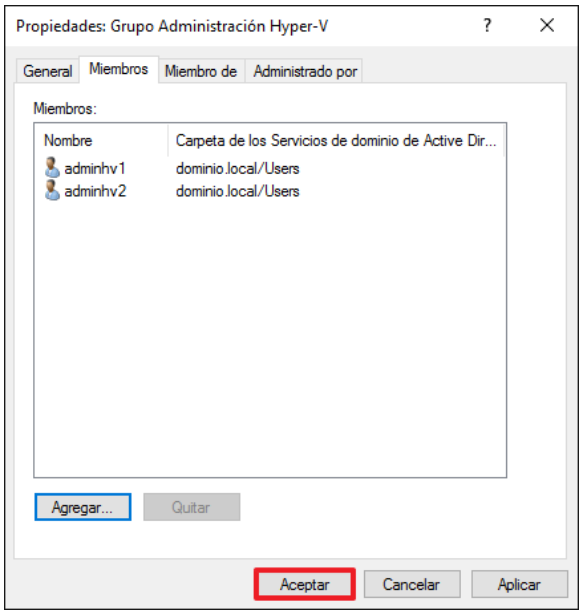
2.10. SEGREGACION DE ROLES

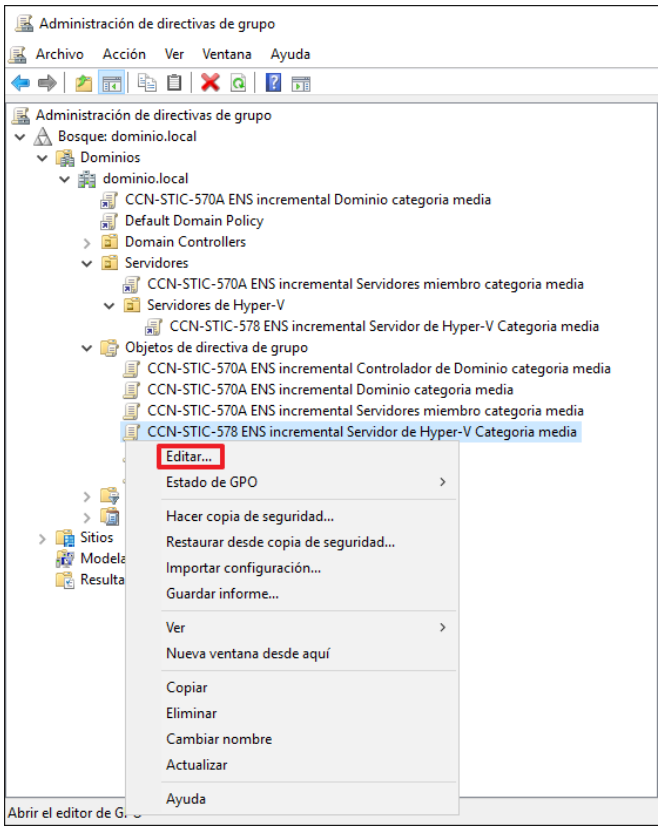
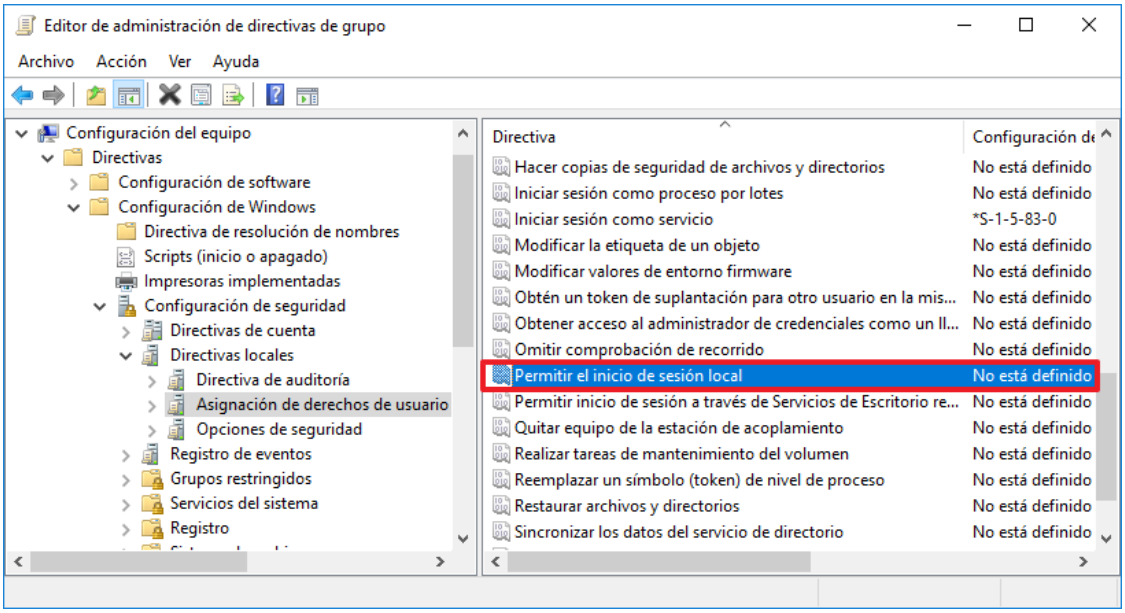
A partir de la aplicación del ENS para la categoría media sobre el Servidor de Hyper-V será necesario crear grupos de usuarios para conceder permisos de administración sobre Hyper-V.

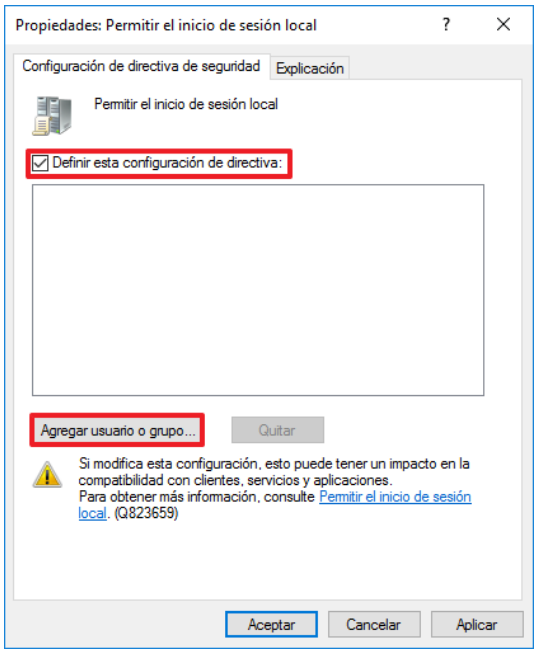
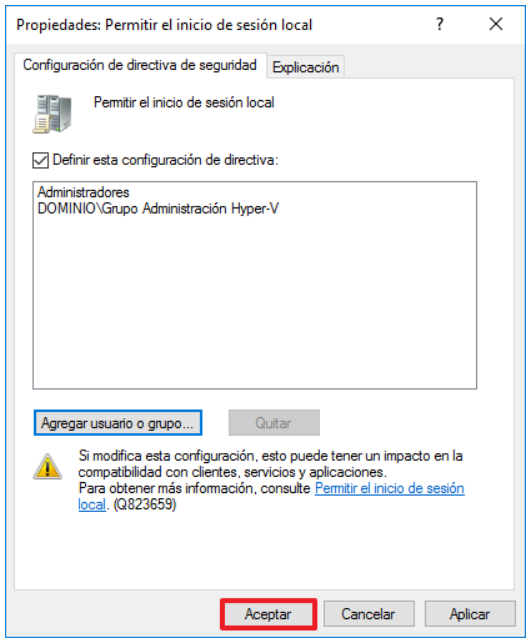
Paso	Descripción
151.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
152.	Ejecute el “Administrador del Servidor” desde el icono correspondiente. 
153.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 

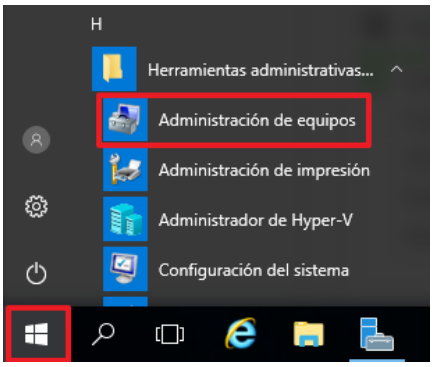
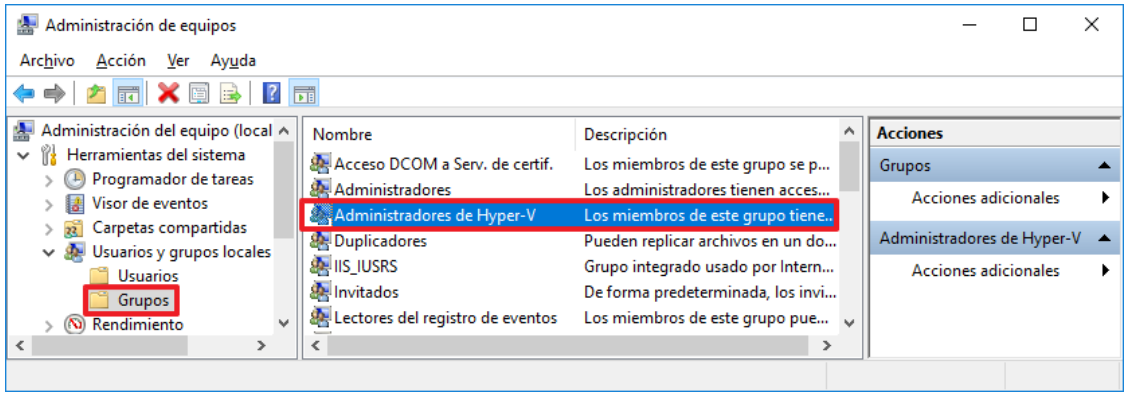
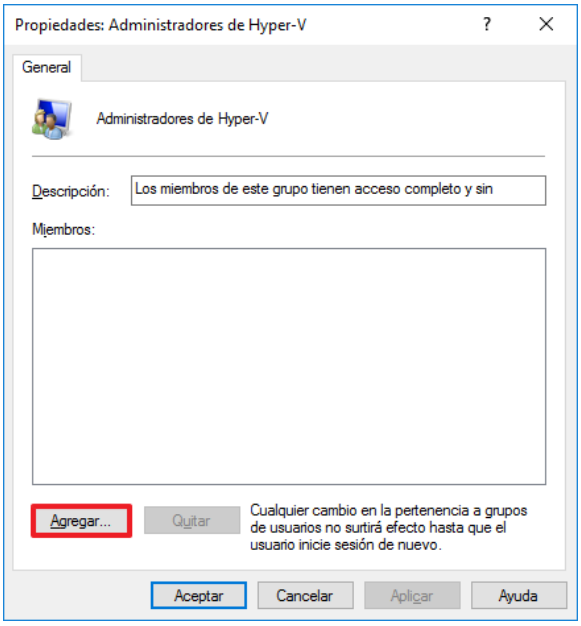
Paso	Descripción
154.	Inicie la herramienta “Usuarios y equipos Active Directory”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Usuarios y equipos de Active Directory”**. 
155.	Despliegue el nodo **“<<su dominio>> → Users”**. Pulse con el botón derecho sobre “Users” y seleccione la opción del menú contextual **“Nuevo → Grupo”**. 

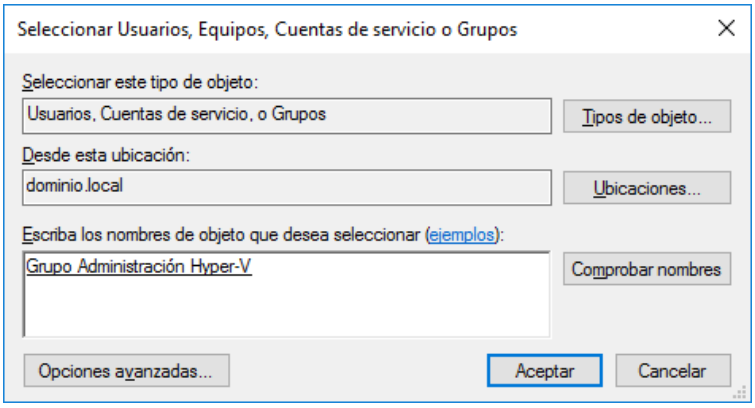
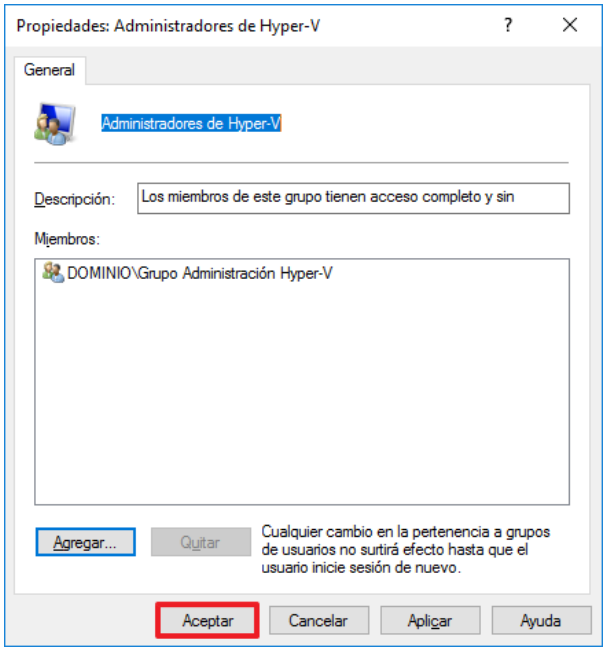
Paso	Descripción
156.	Establezca el nombre de grupo deseado para su organización y pulse “Aceptar”.  **Nota:** En este ejemplo se utiliza el nombre “Grupo Administración Hyper-V”.
157.	Haga doble clic sobre el grupo recién creado y acceda a la pestaña “Miembros”. Pulse sobre el botón “Agregar…” para añadir usuarios al grupo. 

Paso	Descripción
158.	Añada los usuarios que desee al grupo y pulse “Aceptar”.  **Nota:** En este ejemplo se añaden los usuarios “adminhv1” y “adminhv2” utilizados para la creación de esta guía.”
159.	Pulse “Aceptar” cuando haya finalizado. 
160.	A continuación, inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor”, abierta en pasos anteriores, seleccione **“Herramientas → Administración de directivas de grupo”.** 

Paso	Descripción
161.	Acceda al nodo “Objetos de directiva de grupo”, pulse con el botón derecho el objeto GPO denominado “CCN-STIC-578 incremental Servidor de Hyper-V Categoria media”, creado en apartados anteriores y seleccione la opción del menú contextual “Editar…”. 
162.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”**. Haga doble clic en el panel derecho sobre la directiva **“Permitir el inicio de sesión local”**. 

Paso	Descripción
163.	Marque la casilla “Definir esta configuración de directiva:” y pulse sobre “Agregar usuario o grupo…”. 
164.	Agregue el grupo “Administradores” y aquellos usuarios o grupos delegados para la administración del servidor de Hyper-V. Pulse “Aceptar” cuando haya finalizado.  **Nota:** En este ejemplo se hace uso del grupo denominado “Grupo Administración Hyper-V”. Deberá adaptar esta configuración a las necesidades de su organización.
165.	A continuación, inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS. **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

Paso	Descripción
166.	Pulse sobre "Inicio" y seleccione **"Herramientas administrativas → Administración de equipos"**. 
167.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar.
168.	Despliegue el nodo **"Administración del equipo (local) → Herramientas del sistema → Usuarios y grupos locales → Grupos"** y haga doble clic sobre el grupo "Administradores de Hyper-V". 
169.	En la ventana emergente pulse sobre "Agregar...". 

Paso	Descripción
170.	Agregue los usuarios o grupo pertenecientes al dominio que tengan como privilegio la administración del servidor de Hyper-V.  **Nota:** En este ejemplo se hace el grupo denominado "Grupo Administración Hyper-V" creado para tal propósito. Los usuarios o grupos aquí introducidos deberán coincidir con lo introducidos en el paso 164 para permitir la administración de lo contrario ésta no será posible.
171.	Cuando haya finalizado pulse "Aceptar" para guardar la configuración. 
172.	A partir de este momento los usuarios perteneciente al grupo definido como "Grupo Administración Hyper-V" podrán acceder al servidor de Hyper-V y administrar dicho rol.

ANEXO A.3.2. LISTA DE COMPROBACIÓN DE HYPER-V SOBRE WINDOWS SERVER 2016 PARA SERVIDORES QUE LES SON DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

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 PARA LA IMPLEMENTACIÓN SEGURA DE HYPER-V SOBRE SERVIDORES WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS".

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

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

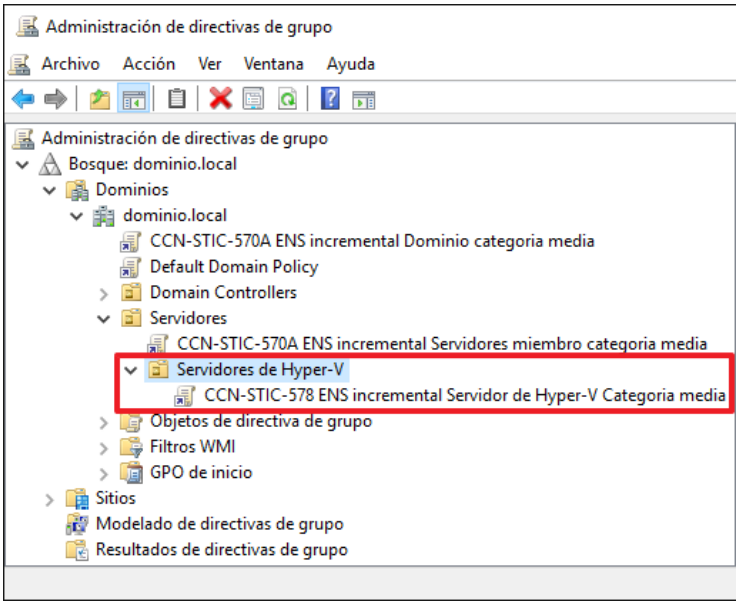
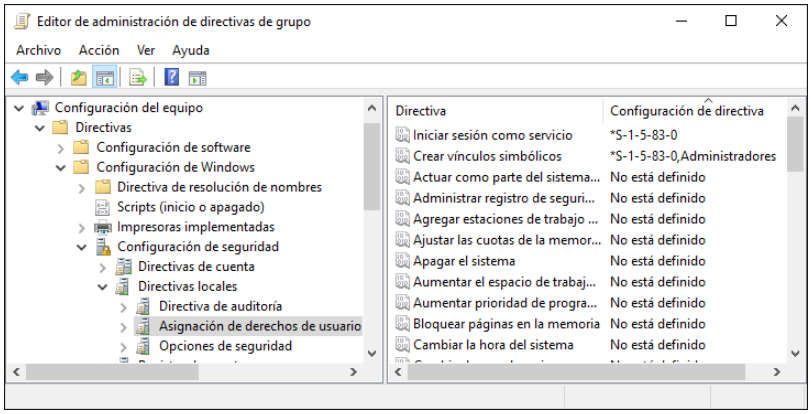
Posteriormente, se deberán realizar las comprobaciones en el propio servidor de Hyper-V, para lo que será necesario ejecutar diferentes consolas de administración y herramientas del sistema, las cuales estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario con privilegios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

a) En el Controlador de Dominio:
   i. Usuarios y equipos de Active Directory (dsa.msc).
   ii. Administrador de directivas de grupo (gpmc.msc).
   iii. Editor de objetos de directiva de grupo (gpedit.msc).

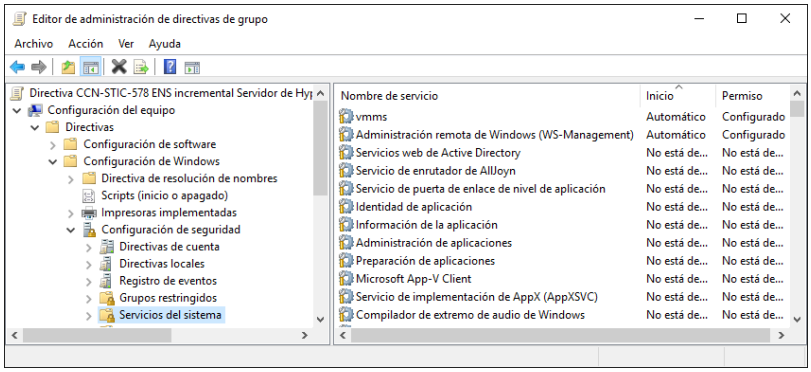
b) En el servidor de Hyper-V:
   i. Administrador de Windows (explorer.exe).
   ii. PowerShell (powershell.exe).
   iii. Servicios (services.msc).
   iv. Editor de objetos de directiva de grupo (gpedit.msc).
   v. Administrador de Hyper-V (virtmgmt.msc).
   vi. Visor de eventos (eventvwr.msc).

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

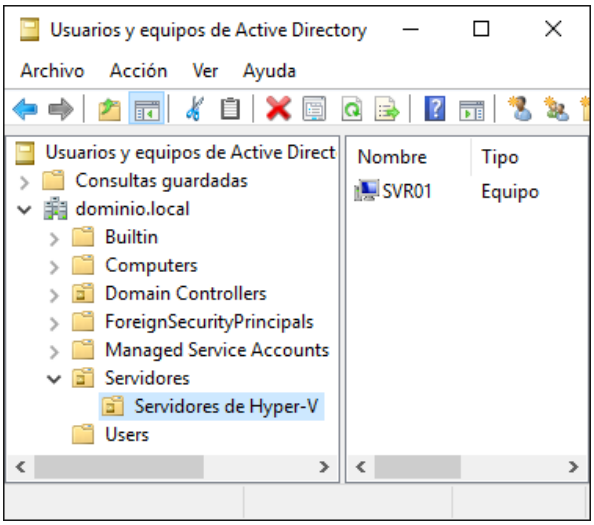
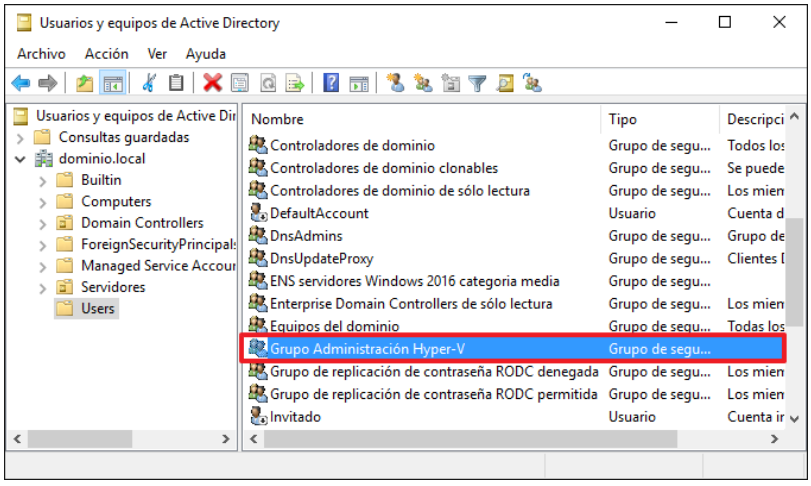
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un Controlador de Dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.

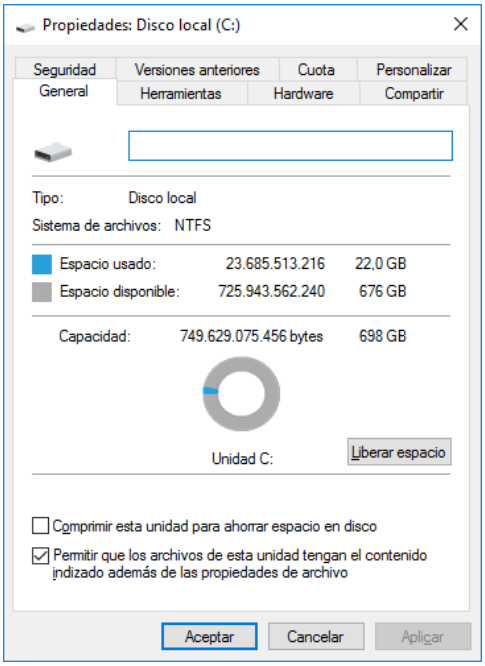
Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que está creada la directiva "CCN-STIC-578 ENS incremental Servidor de Hyper-V Categoria media".		Utilice el Administrador de directivas de grupo (**Inicio → Herramientas administrativas → Administración de directivas de grupo**) y despliegue el menú en árbol hasta llegar a la unidad organizativa "Servidores de Hyper-V" que se encuentra en la Unidad Organizativa "Servidores". Verifique que está creada la política "CCN-STIC-578 ENS incremental Servidor de Hyper-V Categoria media". 
3. Verifique los valores de la asignación de derechos de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria media" tiene los siguientes valores de asignación de derechos de usuario en el siguiente nodo: **Directiva CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario.** 

Directiva	Valor	OK/NOK
Iniciar sesión como servicio	Máquinas virtuales (*S-1-5-83-0)	
Crear vínculos simbólicos	Máquinas virtuales (*S-1-5-83-0) Administradores	

Comprobación	OK/NOK	Cómo hacerlo
4. Verifique los valores de servicios.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria media" tiene los siguientes valores de asignación de derechos de usuario en el siguiente nodo: **Directiva CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del Sistema.** 

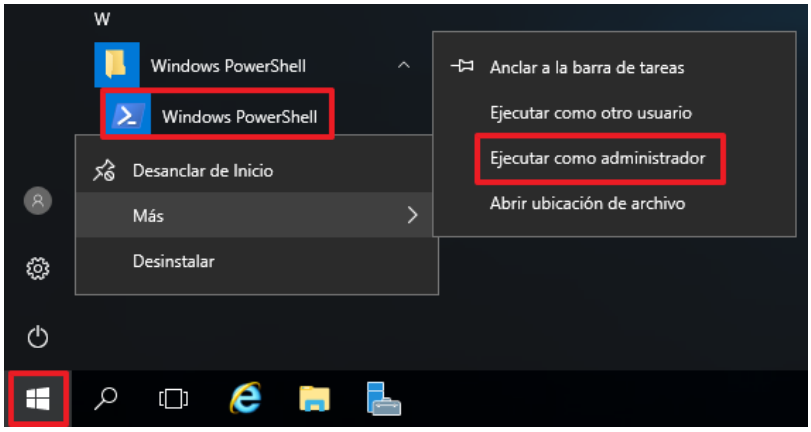
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Administración de máquinas virtuales de Hyper-V	vmms	Automático	Configurado	
Agente de host NC	nchostagent	Deshabilitado	Configurado	
Aislamiento de claves CNG	keyiso	Automático	Configurado	
Instantáneas de volumen	vss	Manual	Configurado	
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado	
Servicio de cierre de invitado de Hyper-V	vmicshutdown	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado	
Servicio de proceso de host de Hyper-V	vmcompute	Manual	Configurado	
Servicio de proxy DNS	DNSProxy	Deshabilitado	Configurado	
Servicio de red de host	hns	Manual	Configurado	
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado	
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual	Configurado	
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado	
Software Load Balancer Host Agent	SlbHostAgent	Manual	Configurado	

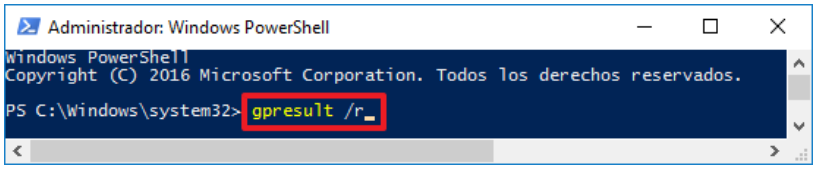
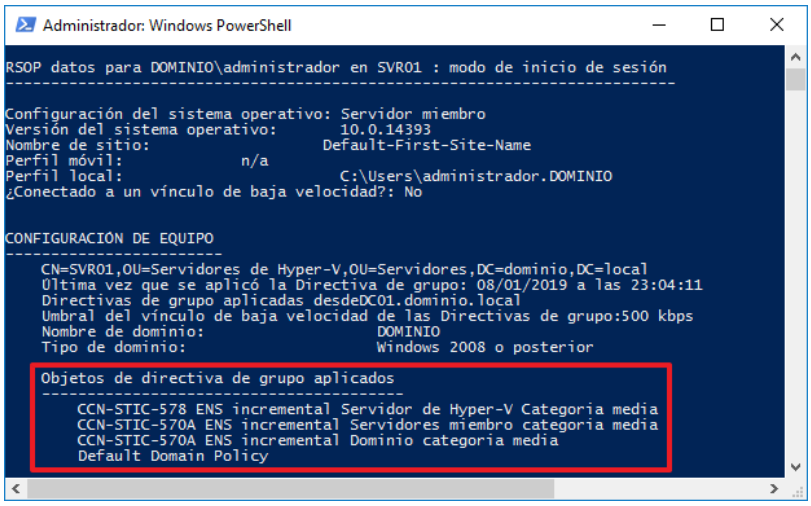
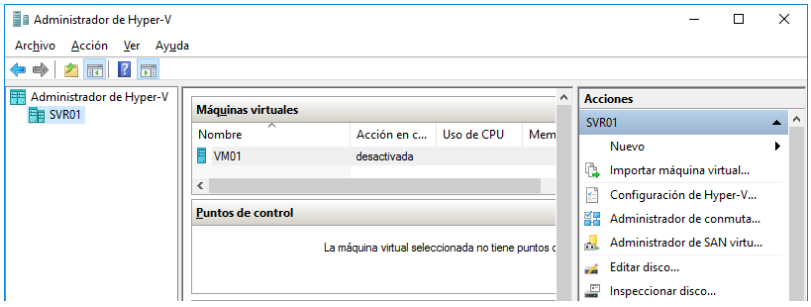
Comprobación	OK/NOK	Cómo hacerlo
5. Verifique que los servidores de Hyper-V están dentro de las Unidades Organizativas adecuada		Utilice la herramienta Usuarios y equipos de Active Directory (**Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**) y seleccione las unidades organizativas que contienen los Servidores de Hyper-V. Compruebe que existe un objeto de tipo equipo por cada uno de los servidores de Hyper-V que se están asegurando.  **Nota:** Para el desarrollo de esta guía se utiliza la Unidad Organizativa "Servidores de Hyper-V".
6. Verifique que existe un grupo dedicado para la administración de Hyper-V		Utilice la herramienta Usuarios y equipos de Active Directory (**Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**) y verifique que existe al menos un grupo dedicado a la administración del Servidor de Hyper-V.  **Nota:** El nombre del grupo y los usuarios pertenecientes al grupo variará dependiendo de la configuración aplicada en su organización

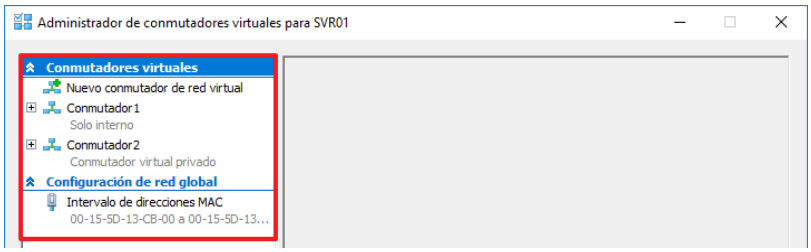
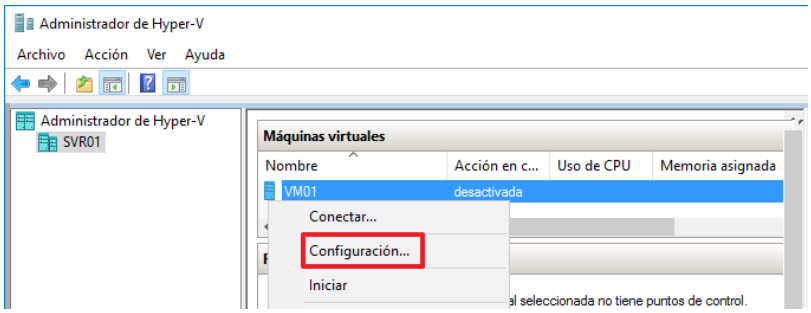
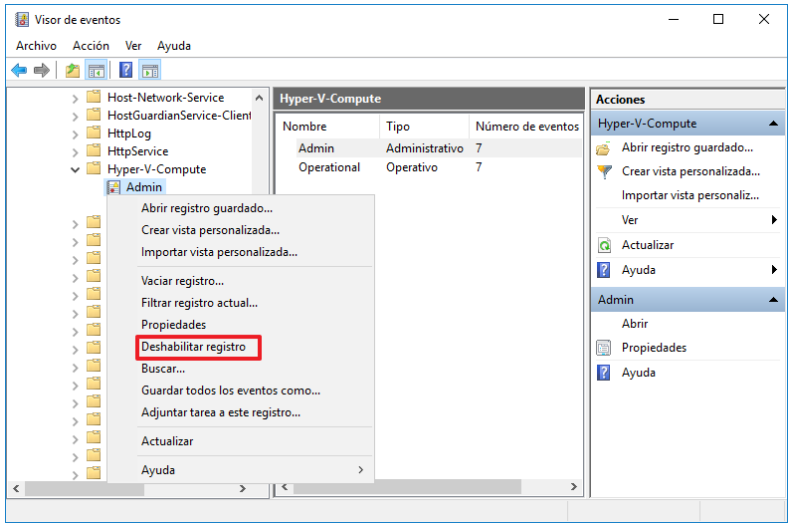
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>7. Inicie sesión en un Servidor de Hyper-V</td><td></td><td>Para completar el resto de la lista de verificación deberá iniciar sesión con una cuenta que tenga permisos de administrador del dominio.</td></tr>
<tr><td>8. Verifique el sistema de ficheros de los volúmenes</td><td></td><td>Utilizando el explorador de Windows (botón derecho sobre Inicio → Explorador de archivos, botón derecho sobre la unidad C:\), verifique en las propiedades de cada partición el uso del sistema de archivos NTFS o cualquier sistema de archivos que permita la aplicación de ACL’s.
 
</td></tr>
<tr><td rowspan="3">9. Verifique que están instalados los componentes que se indican</td><td></td><td>En el “Administrador del Servidor”, pulse sobre la opción “Servidor Local” situado en el lateral izquierdo y diríjase a la parte final de la ventana principal, “Roles y características”, por medio del scroll lateral derecho.
Compruebe que se encuentran instalados los siguientes componentes.</td></tr>
<tr><td colspan="2">Rol</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Hyper-V</td><td></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
10. Verifique los valores de servicios.		Ejecute el complemento "Servicios" (ejecutando "services.msc" desde **"Inicio → Ejecutar…"**) y compruebe el tipo de inicio de los servicios que se indican a continuación.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Administración de máquinas virtuales de Hyper-V	vmms	Automático	Configurado	
Agente de host NC	nchostagent	Deshabilitado	Configurado	
Aislamiento de claves CNG	keyiso	Automático	Configurado	
Instantáneas de volumen	vss	Manual	Configurado	
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado	
Servicio de cierre de invitado de Hyper-V	vmicshutdown	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado	
Servicio de proceso de host de Hyper-V	vmcompute	Manual	Configurado	
Servicio de proxy DNS	DNSProxy	Deshabilitado	Configurado	
Servicio de red de host	hns	Manual	Configurado	
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado	
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual	Configurado	
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado	
Software Load Balancer Host Agent	SlbHostAgent	Manual	Configurado	

11. Inicie la consola de PowerShell		Ejecute la consola de PowerShell. Para ello pulse sobre "Inicio", seleccione **"Windows Powershell → Windows Powershell"** con el botón derecho y pulse sobre la opción **"Más → Ejecutar como administrador"**. 

Comprobación	OK/NOK	Cómo hacerlo
12. Verifique que se están aplicando los objetos GPO necesarios		Verifique que se estan aplicando las GPOs correspondientes ejecutando el comando “gpresult /r”. 
13. Verifique que se están aplicando los objetos GPO necesarios		Verifique que se aplican los siguientes objetos GPO y en el siguiente orden. – CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria media. – CCN-STIC-570A ENS incremental Servidores miembro categoria media. – CCN-STIC-570A ENS incremental Dominio categoria media. 
14. Verifique que la instalación se ha realizado correctamente		Utilizando la herramienta de administración de Hyper-V (ejecutando “virtmgmt.msc” desde **Inicio → Ejecutar…**), verifique que la consola se inicia y presenta el servidor local como un servidor de Hyper-V. 

Comprobación	OK/NOK	Cómo hacerlo
15. Verifique que se disponen de conmutadores de red virtuales configurados		Utilizando la herramienta de administración de Hyper-V (ejecutando "virtmgmt.msc" desde **Inicio → Ejecutar…**), verifique haciendo uso de la opción "Administrador de conmutadores virtuales" del panel de acciones, que existen conmutadores virtuales configurados. 
16. Verifique que existen máquinas y que su configuración es adecuada		Utilizando la herramienta de administración de Hyper-V (ejecutando "virtmgmt.msc" desde **Inicio → Ejecutar…**), verifique que existen máquinas virtuales y que estas poseen la configuración adecuada haciendo clic derecho sobre cada una de ellas y seleccionando la opción del menú contextual "Configuración". 
17. Verifique que la auditoría sobre el servidor de Hyper-V se encuentra activada		Utilizando la herramienta de visor de eventos de Windows (ejecutando "eventvwr.msc" desde **Inicio → Ejecutar…**), verifique que la auditoría del servidor de Hyper-V se encuentra activada en todos sus componentes haciendo clic derecho sobre cada uno de sus registros. 

ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.4.1. PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE HYPER-V SOBRE SERVIDORES WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen servidores de virtualización Hyper-V con una categorización de seguridad alta según los criterios del Esquema Nacional de Seguridad.

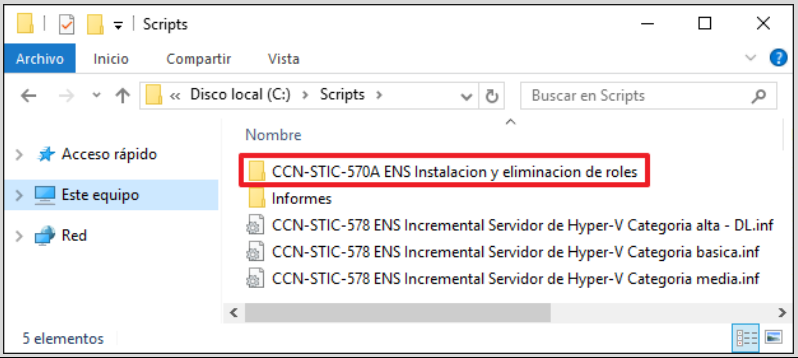
Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios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

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

Nota: Si instala el Servidor de Hyper-V por primera vez con la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016 aplicada debe habilitar la instalación remota de roles características y servicios de rol a través de Shell la cual se encuentra deshabilitada por GPO.
En la guía mencionada anteriormente se describe el procedimiento para implementar el objeto GPO que permite la instalación de roles y características. En caso de no disponer de los datos adjuntos a la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016" encontrará una copia de seguridad para poder importar la GPO necesaria en la carpeta "Scripts" adjunta a la presente guía.

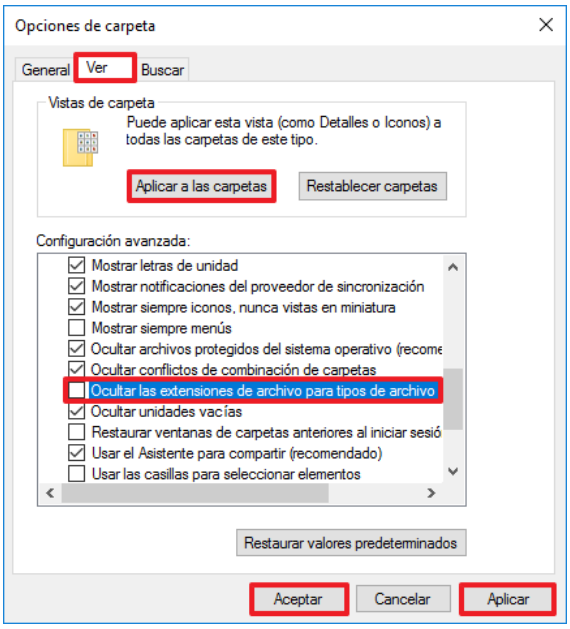
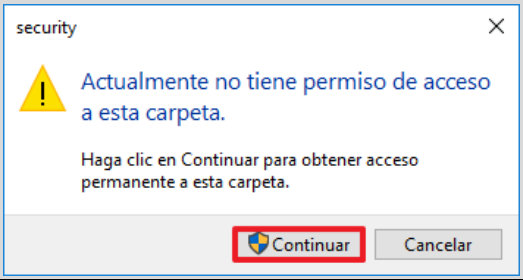


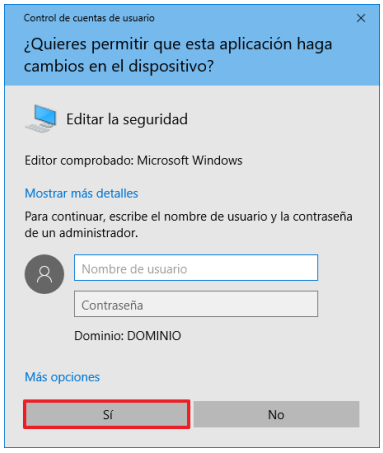
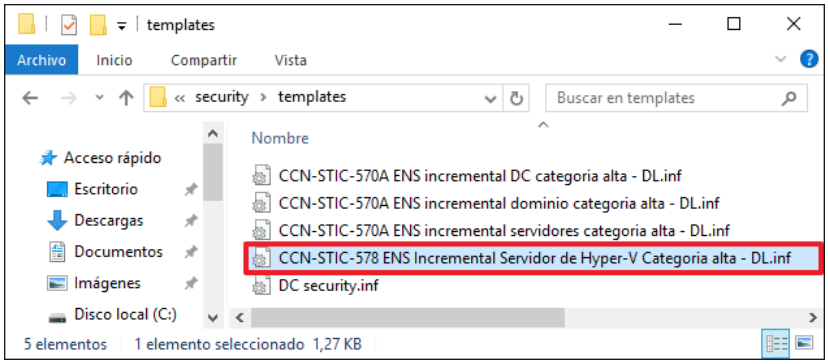
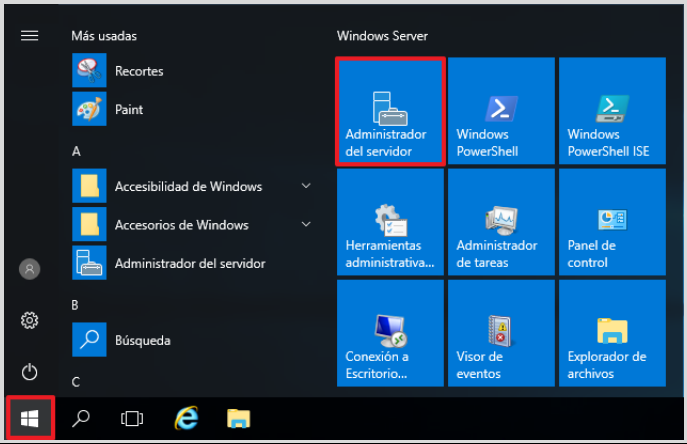
1. PREPARACIÓN DEL DOMINIO

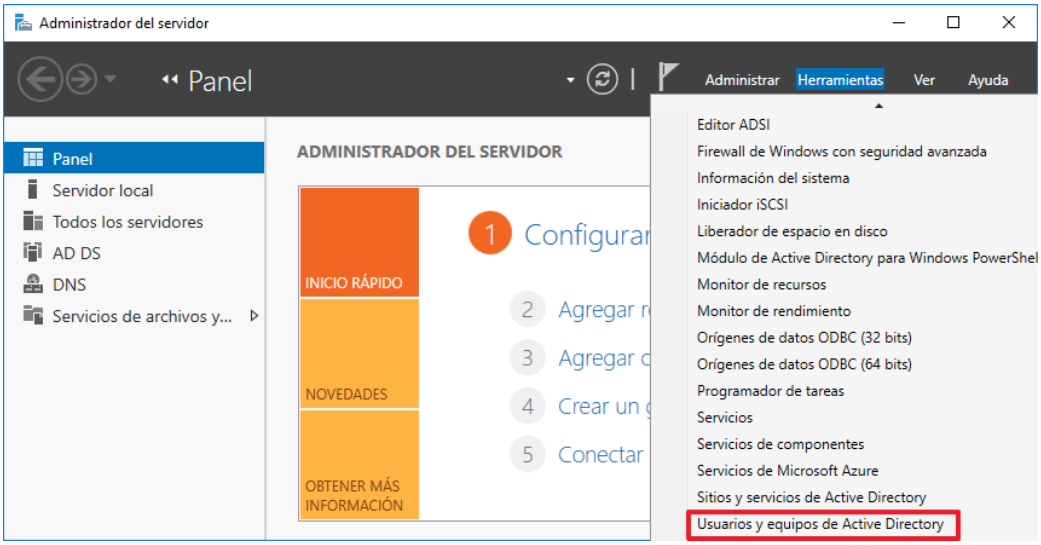
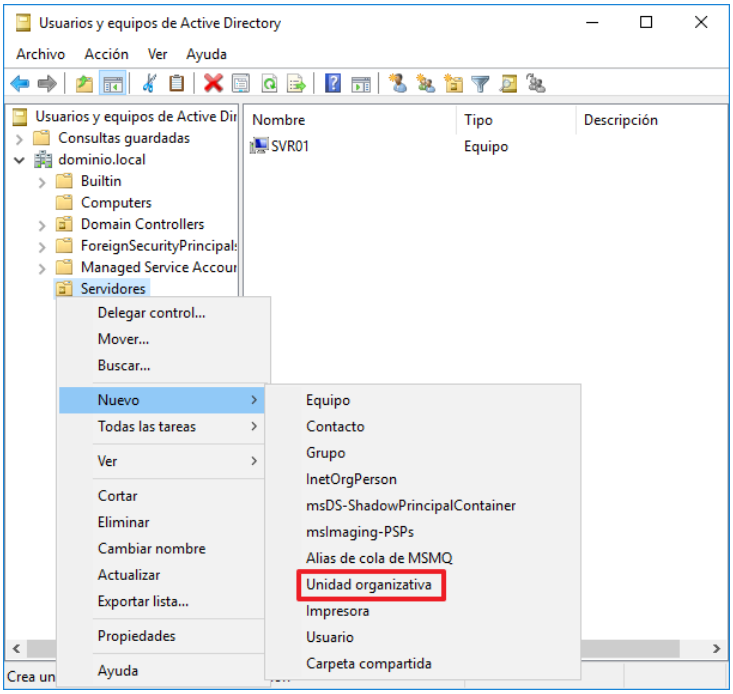
Los pasos que se describen a continuación deberá realizarlos en un Controlador de Dominio del dominio al que pertenece el equipo servidor que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer servidor de Hyper-V que actúe como miembro del dominio. Durante este procedimiento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

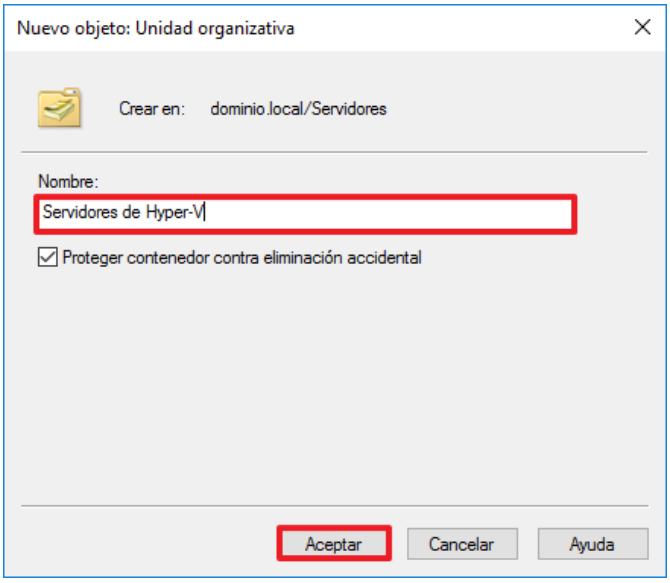
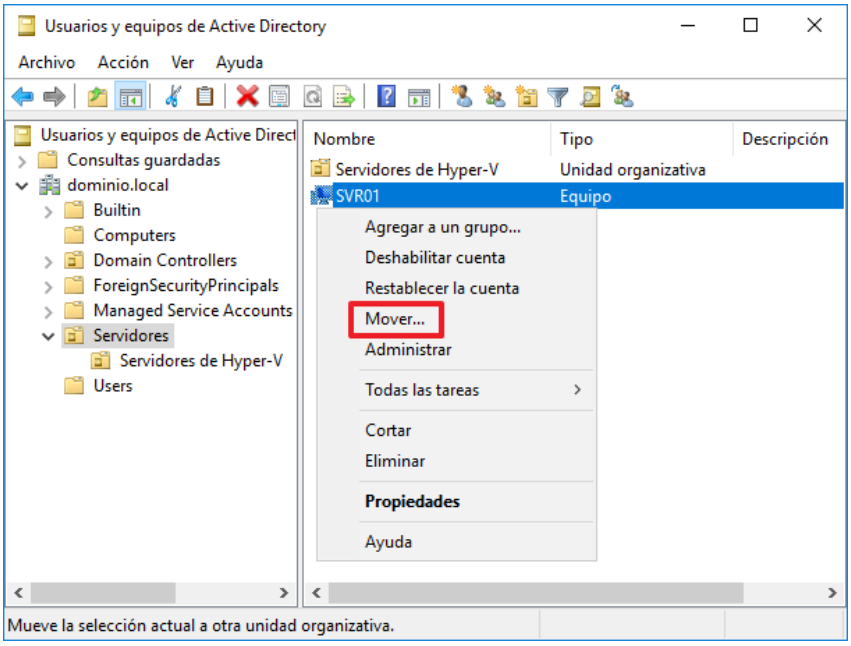
Nota: Esta guía asume que los servidores Controladores del Dominio al que pertenece el equipo servidor de Hyper-V que está asegurando, se les ha aplicado la configuración descrita en la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016". Si no es así, aplique la guía correspondiente al Controlador de Dominio, antes de continuar con la aplicación de ésta.

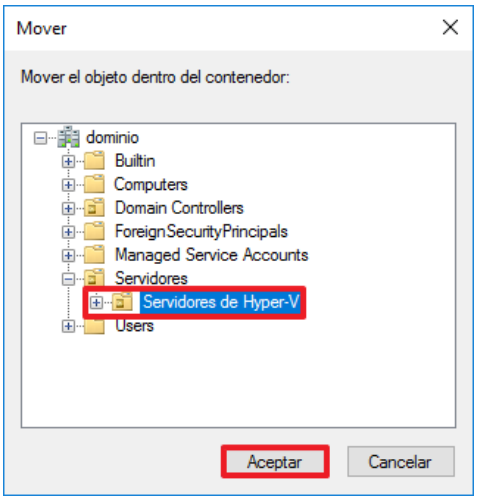
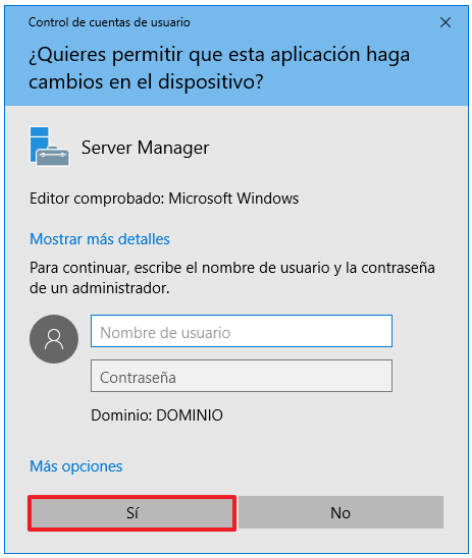
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
2.	Cree el directorio "Scripts" en la unidad "C:\". **Nota:** Los scripts asumen que su ubicación en el sistema será bajo "C:\Scripts". Si los colocara en otra ubicación, tendrá que editar los scripts para reflejar la nueva ubicación.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".
4.	Si no lo ha hecho anteriormente, configure el "Explorador de Windows" para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que "Explorador de Windows" muestra las extensiones de los archivos.

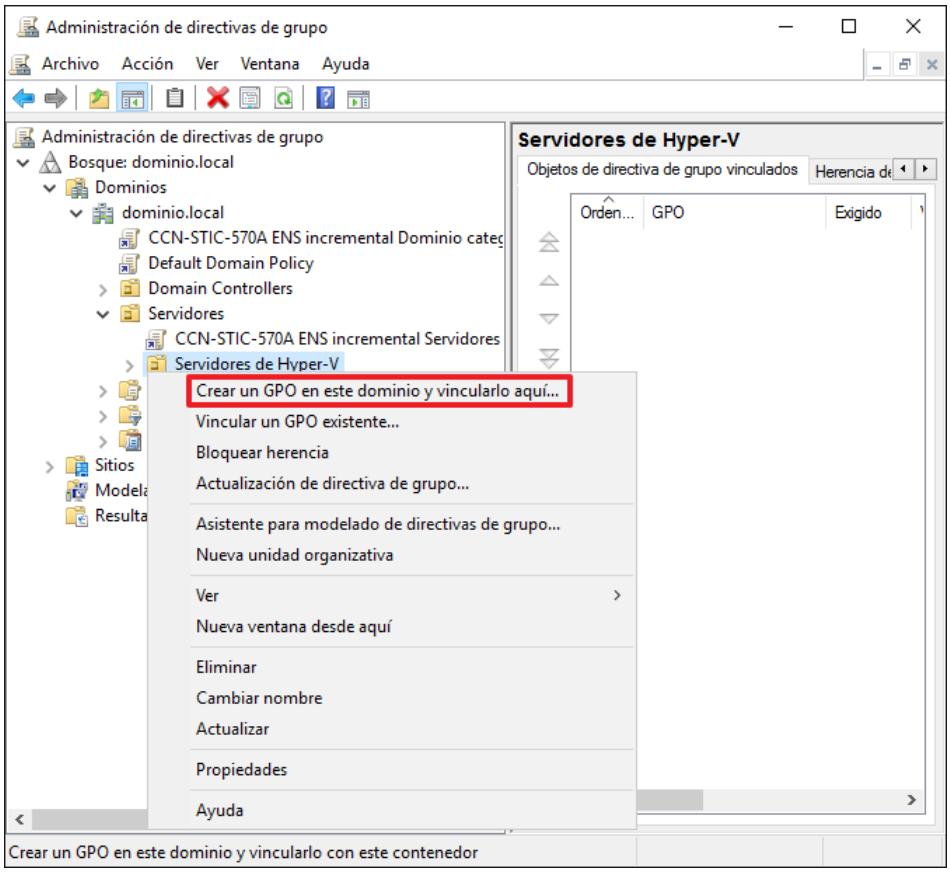
Paso	Descripción
5.	Para configurar el “Explorador de Windows” y que éste muestre las extensiones de todos los archivos, abra una ventana del “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. En la venta emergente, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la imagen.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación “¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?”, y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".
6.	Adicionalmente acceda al directorio “C:\Windows\Security\Templates”. **Nota:** Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón “Continuar” ante la ventana emergente. 

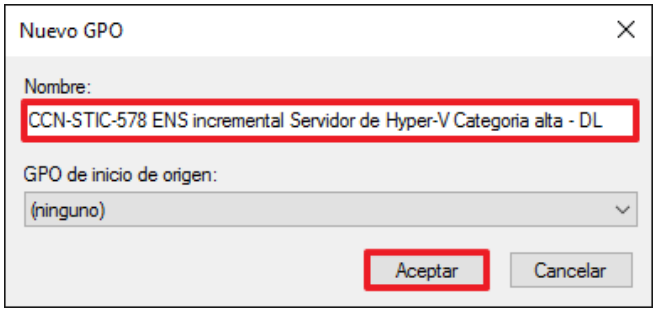
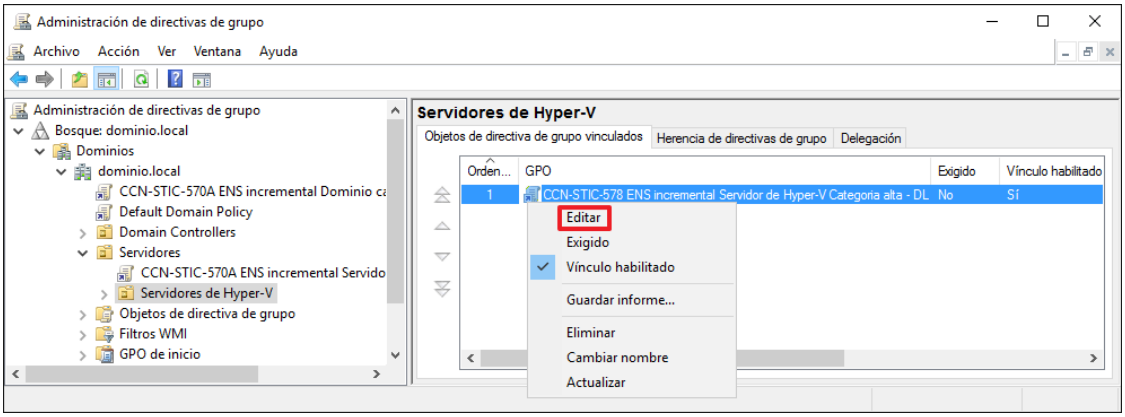
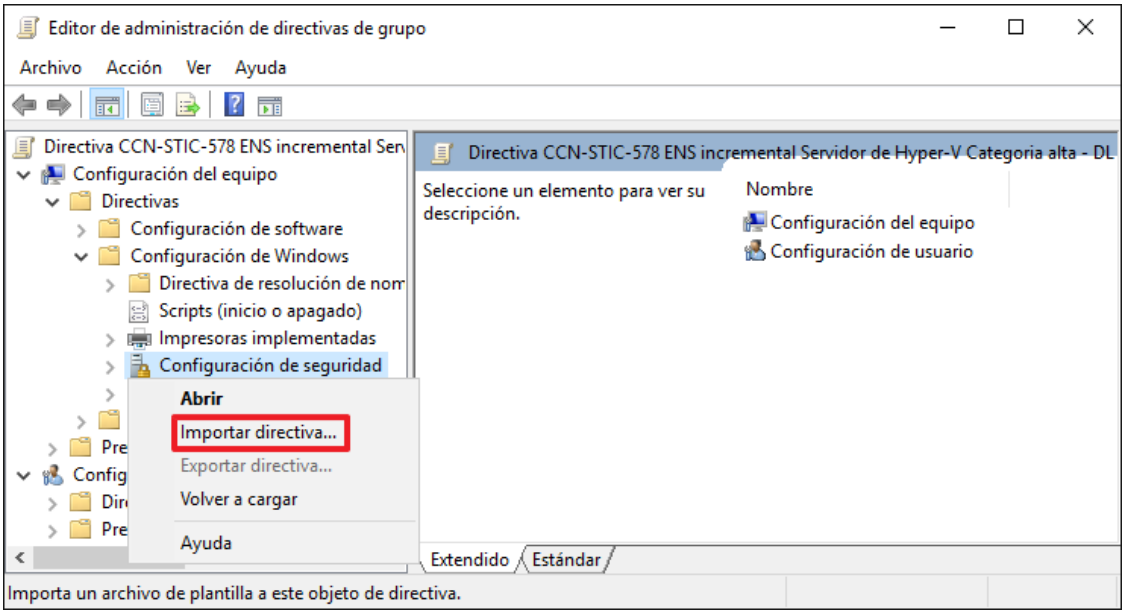
Paso	Descripción
7.	El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar. 
8.	Copie el fichero “CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria alta - DL.inf” ubicado en “C:\Scripts” en el directorio “C:\Windows\Security\Templates”. 
9.	A continuación, deberá crear la unidad organizativa "Servidores de Hyper-V". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente.  **Nota:** Por defecto el “Administrador del servidor” se inicia cuando un usuario inicia sesión en el equipo. Si no se encuentra vinculado a la barrada de tareas podrá acceder a él en la ruta **“Inicio → Administrador del servidor”**. 

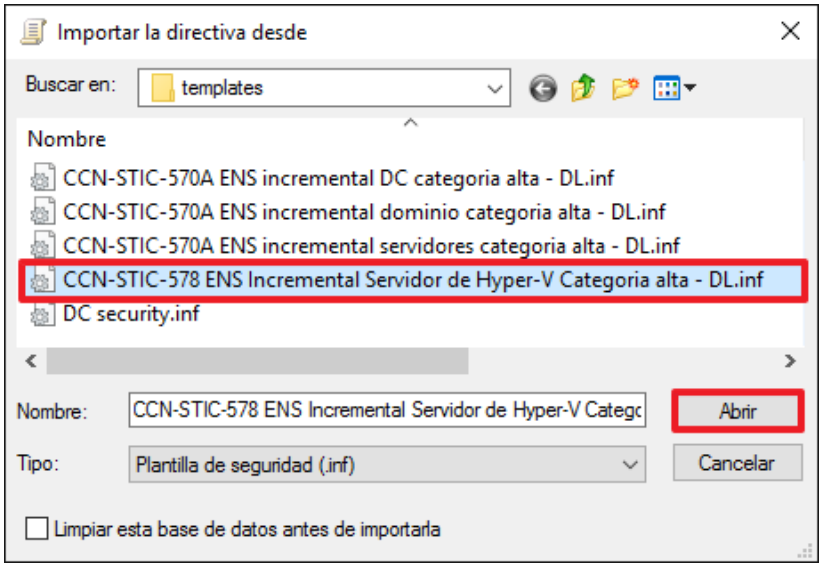
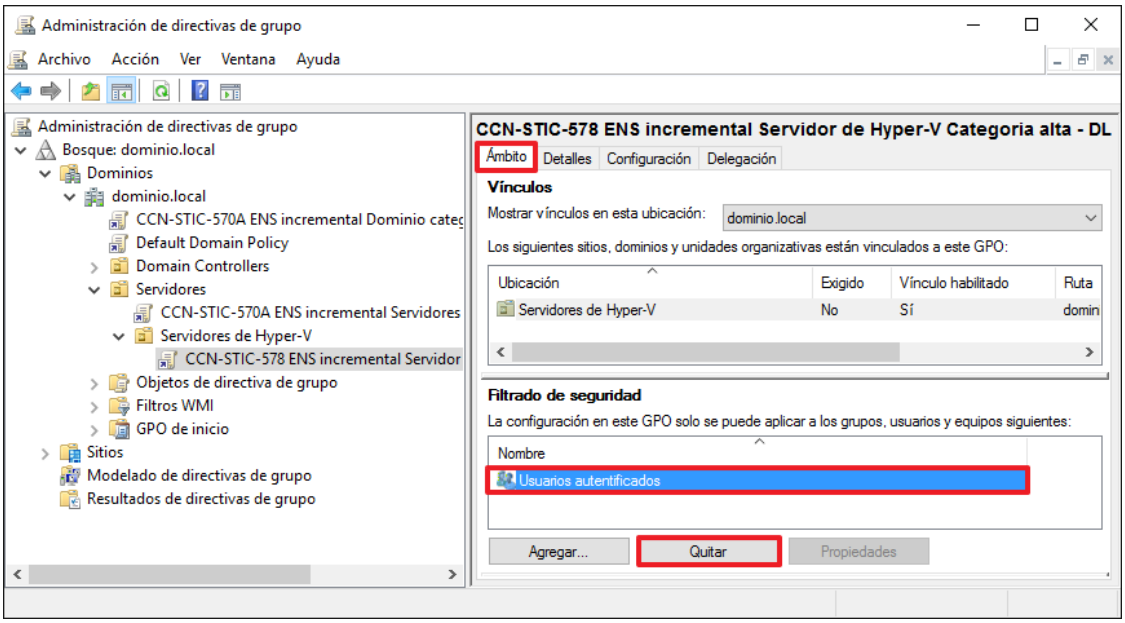
Paso	Descripción
10.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar.
11.	Inicie la herramienta "Usuarios y equipos Active Directory". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Usuarios y equipos de Active Directory"**. 
12.	En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo **"<<dominio>> → <<unidad organizativa>>"**, y desplegando el menú contextual con el botón derecho, seleccione la opción **"Nuevo → Unidad organizativa"**.  **Nota:** En este ejemplo, la unidad organizativa de servidores se encuentra en el nodo **"dominio.local → Servidores"**.

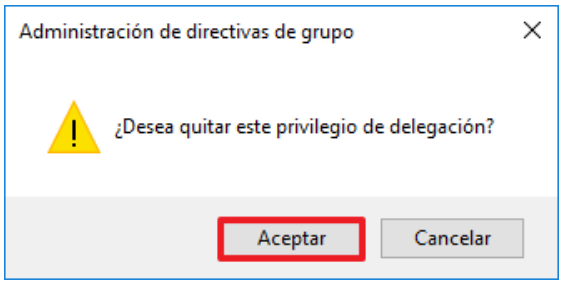
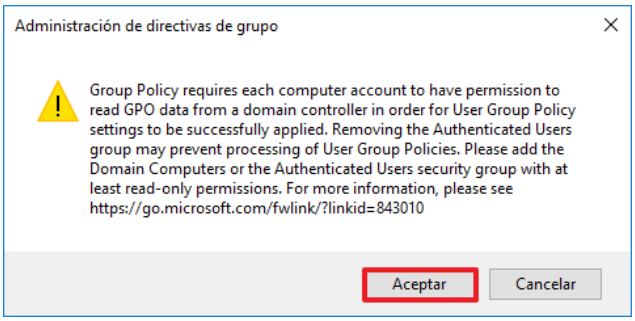
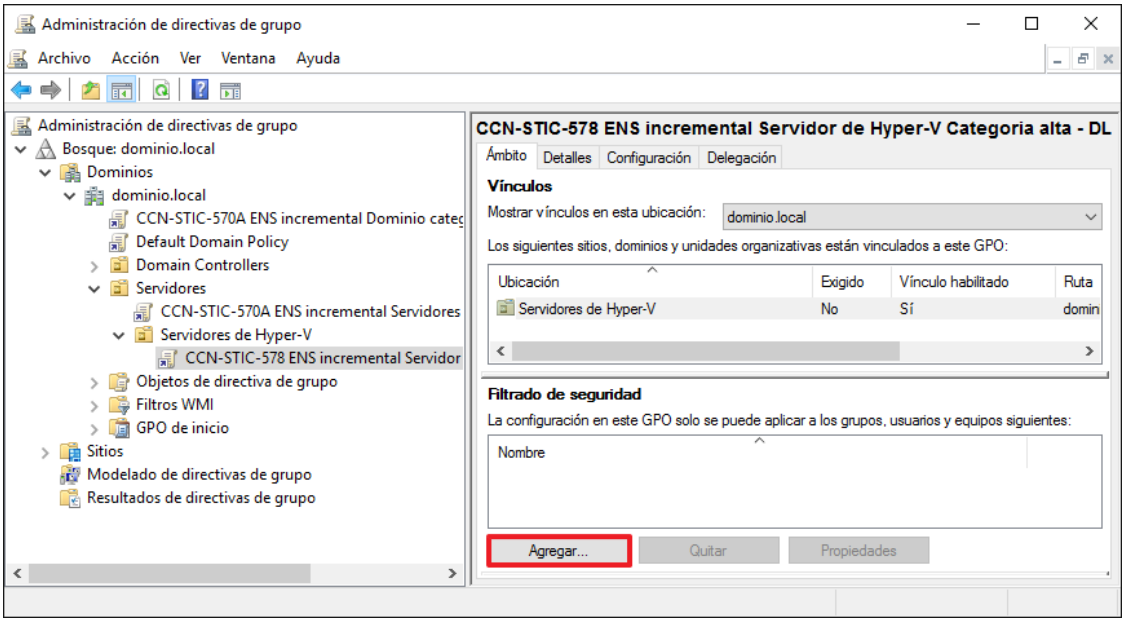
Paso	Descripción
13.	Introduzca el nombre “Servidores de Hyper-V” tal y como se muestra en la imagen y pulse sobre “Aceptar”. 
14.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores de virtualización a la unidad organizativa “Servidores de Hyper-V”. Para ello, haga clic con el botón derecho sobre el equipo que desee reubicar y seleccione la opción del menú contextual “Mover...”. 

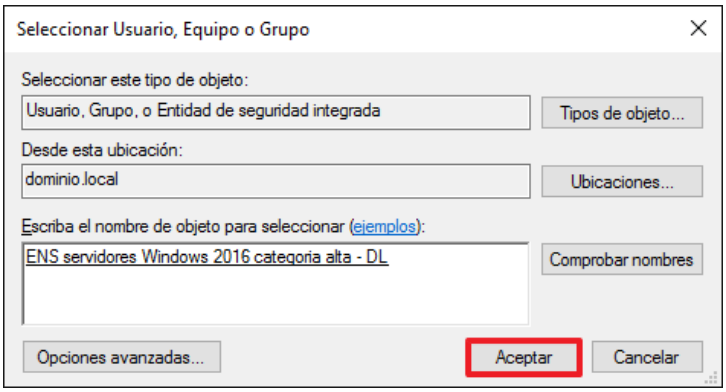
Paso	Descripción
15.	A continuación, seleccione la unidad organizativa “Servidores de Hyper-V” y pulse “Aceptar”. 
16.	Cierre la herramienta “Usuarios y equipos de Active Directory”.
17.	A continuación, deberá crear la GPO "CCN-STIC-578 ENS incremental Servidor de Hyper-V categoria alta - DL". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 
18.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 

Paso	Descripción
19.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administración de directivas de grupo”.** 
20.	A continuación, despliegue el nodo **“Bosque: <<nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores de Hyper-V”**. **Nota:** En este ejemplo el nombre de la unidad organizativa donde se encuentran todos los servidores que implementan este rol, “Servidores de Hyper-V”.
21.	Pulse con el botón derecho sobre la unidad organizativa “Servidores de Hyper-V” y seleccione “Crear un GPO en este dominio y vincularlo aquí…”. 

Paso	Descripción
22.	Introduzca el nombre del objeto GPO, “CCN-STIC-578 ENS incremental Servidor de Hyper-V Categoria alta - DL” y haga clic en el botón “Aceptar”. 
23.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
24.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**.
25.	Pulse con el botón derecho sobre “Configuración de seguridad” y seleccione la opción “Importar directiva…”. 

Paso	Descripción
26.	Seleccione de la ruta "C:\Windows\Security\Templates" el fichero "CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria alta - DL.inf" y pulse el botón "Abrir". 
27.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
28.	Seleccione la nueva política de grupo configurada y vaya a la pestaña "Ámbito" que se encuentra en el panel derecho. En la opción "Filtrado de seguridad", seleccione "Usuarios autentificados" y pulse la opción "Quitar". 

Paso	Descripción
29.	Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”. 
30.	Pulse de nuevo “Aceptar” ante el mensaje de advertencia emergente. 
31.	A continuación, pulse el botón “Agregar…”. 

Paso	Descripción
32.	Introduzca como nombre “ENS Servidores Windows 2016 categoria alta - DL”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A Implementación del ENS en Windows Server 2016”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado, deberá adaptar estos pasos a las necesidades de su organización.

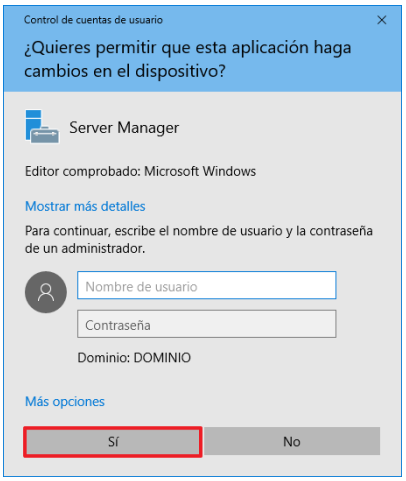
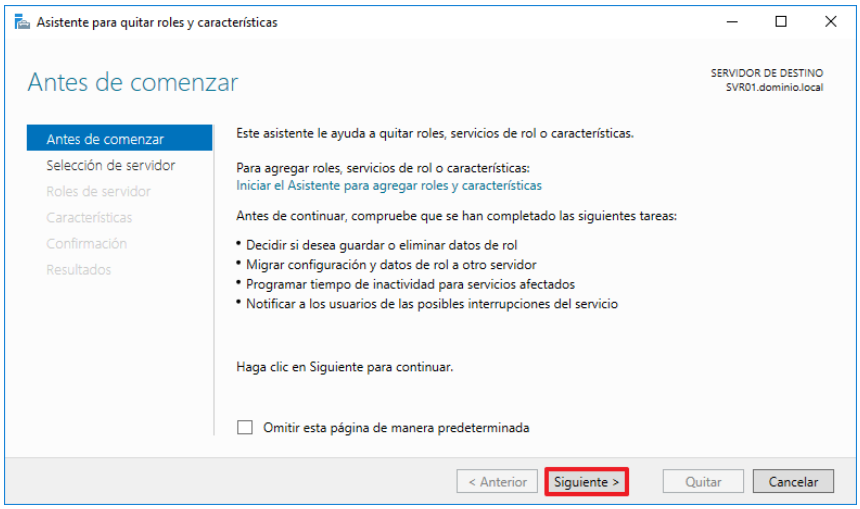
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

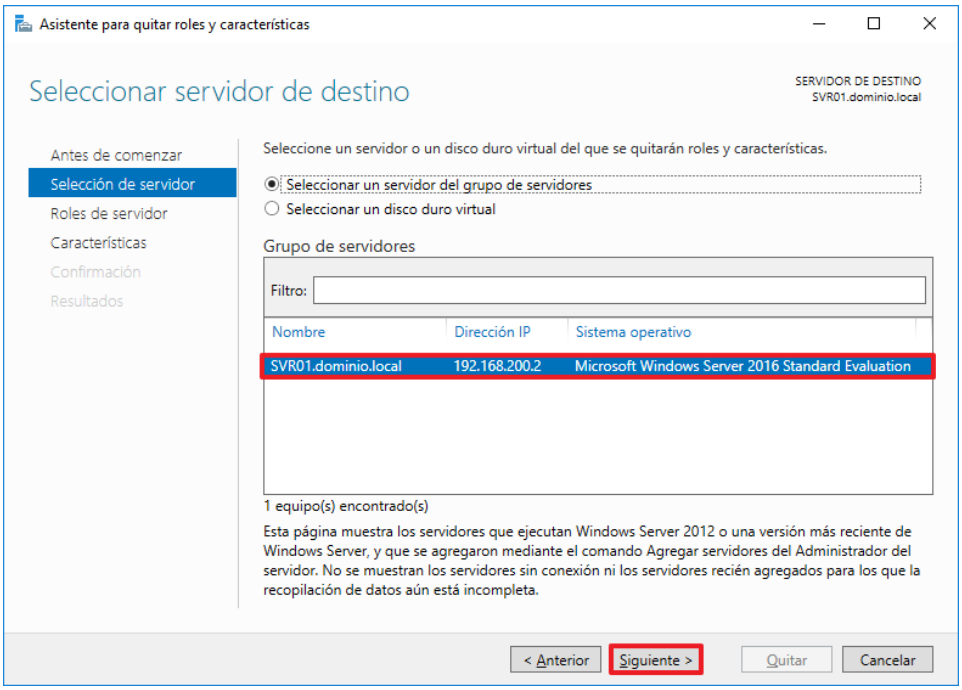
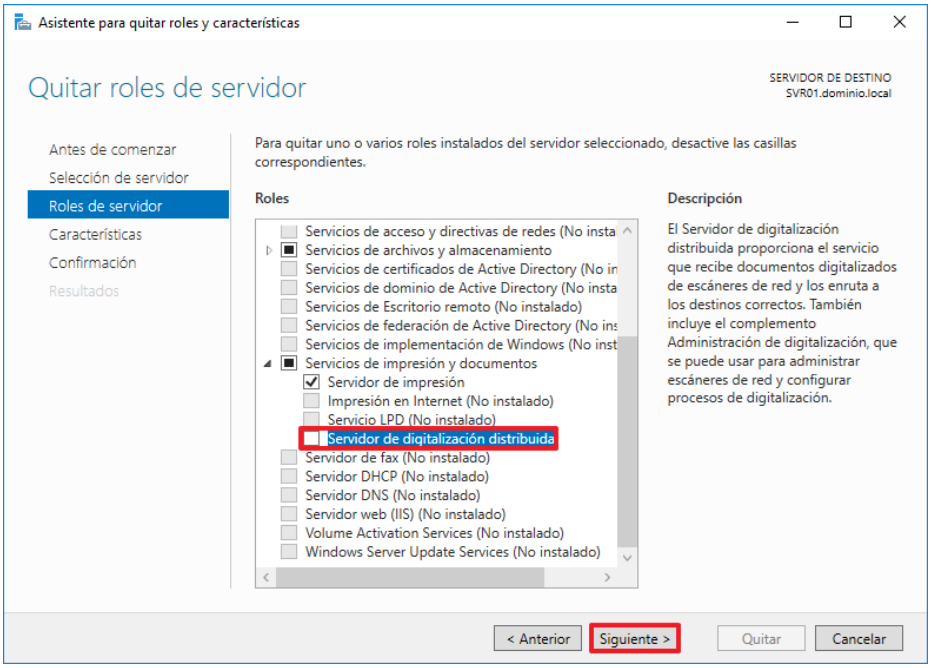
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

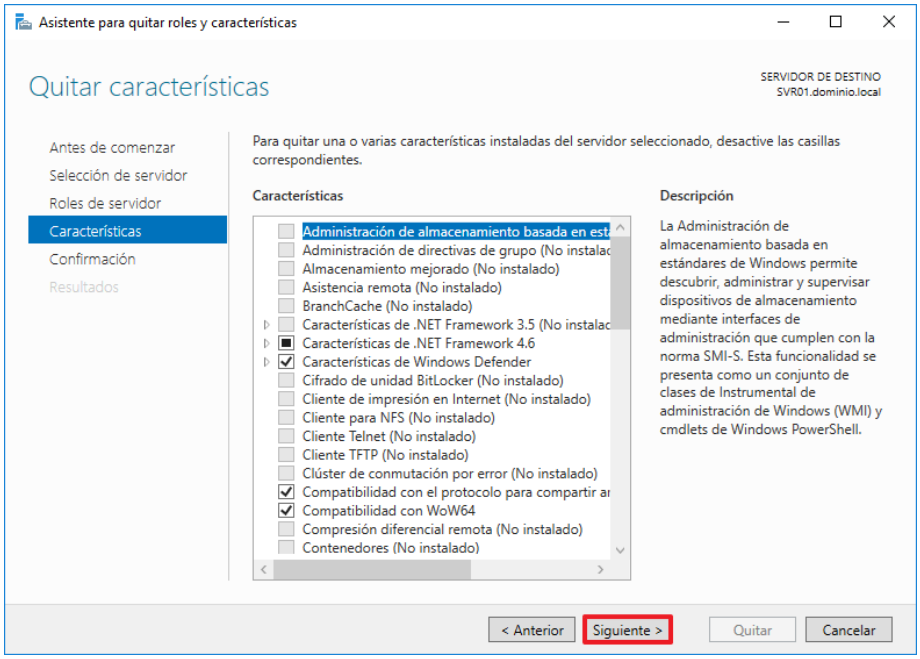
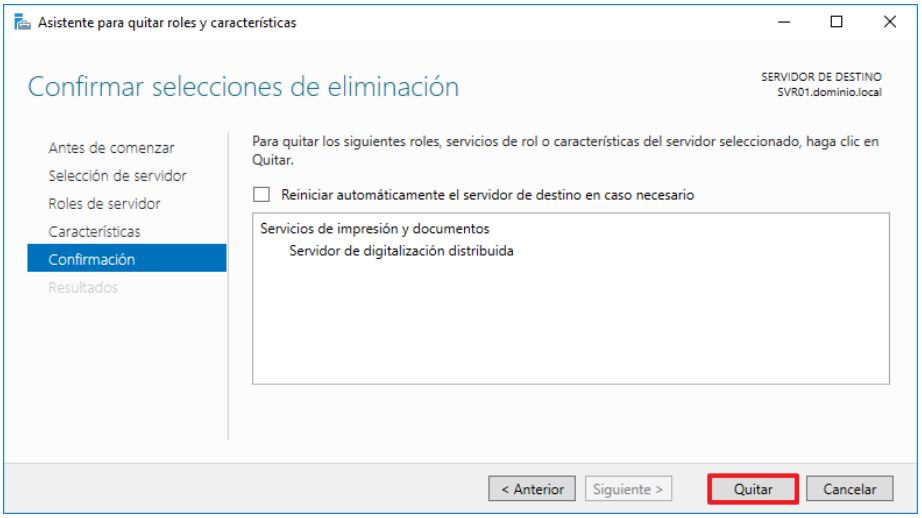
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

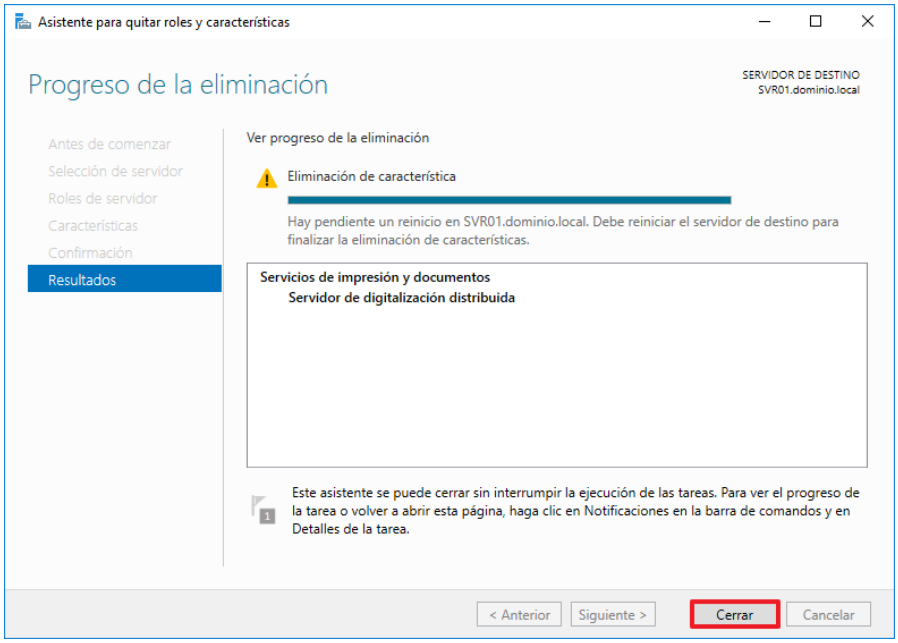
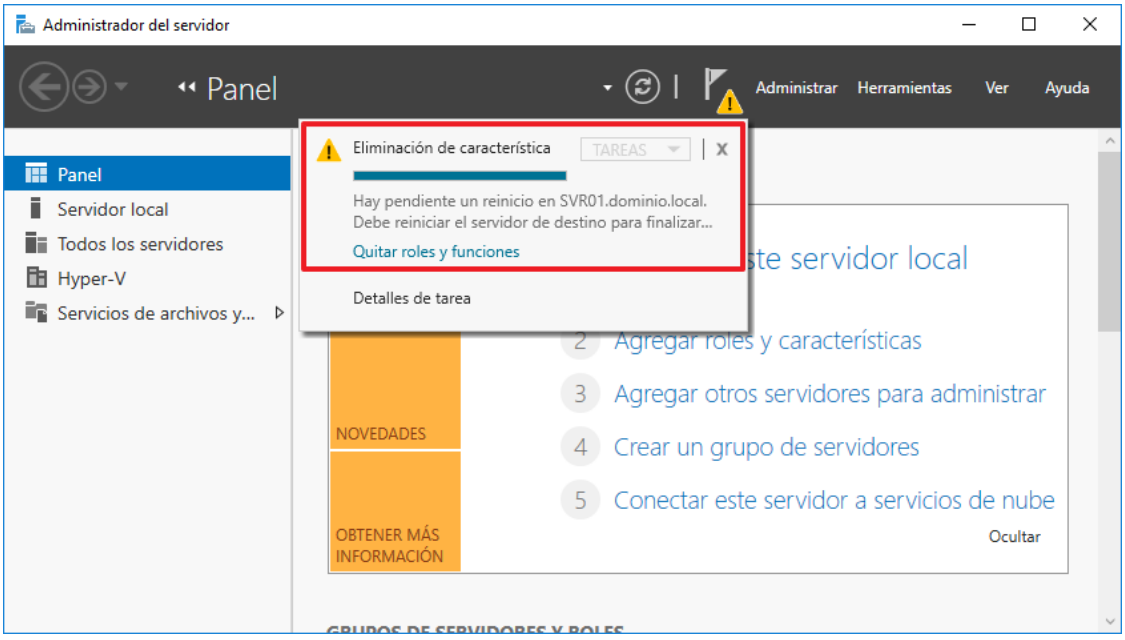
En el procedimiento que se describe a continuación, a modo de ejemplo, desinstala un rol que actualmente no está siendo utilizado por el Servidor de Hyper-V.

Paso	Descripción
33.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

Paso	Descripción
34.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
35.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
36.	A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”. 
37.	Se lanzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 

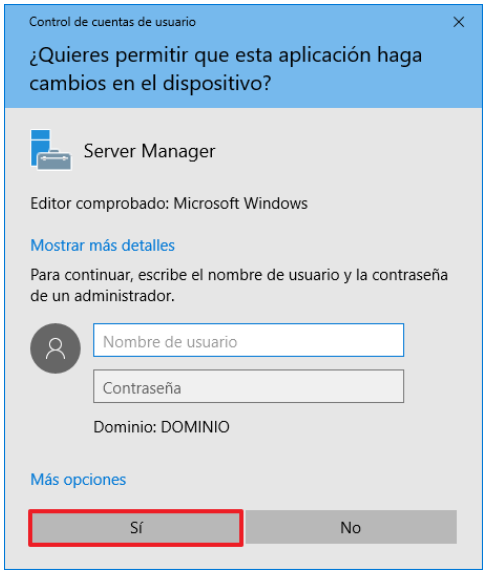
Paso	Descripción
38.	Seleccione el servidor sobre el cual desea eliminar un rol o característica y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “SVR01”.
39.	En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se desinstala el rol “Servidor de digitalización distribuida”.

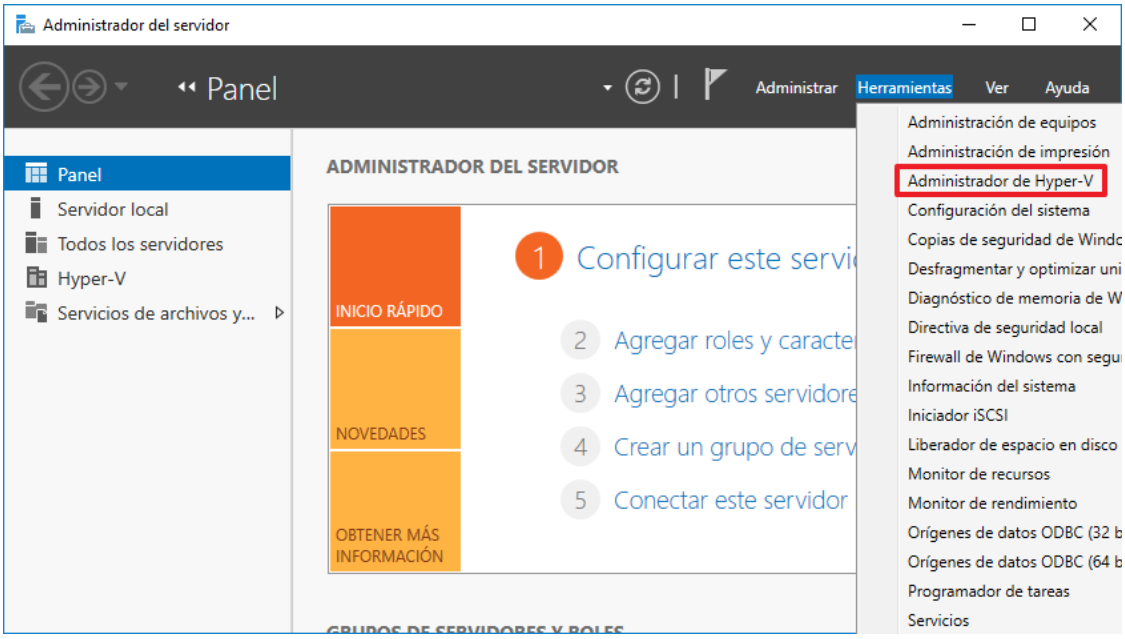
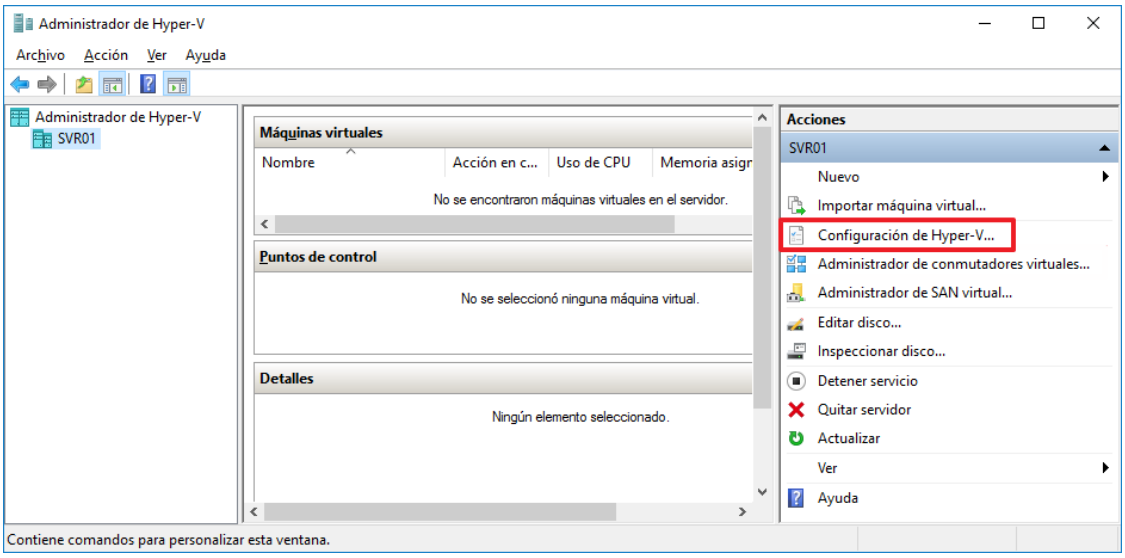
Paso	Descripción
40.	En la ventana de características pulse el botón “Siguiente >”. En este ejemplo no se desinstala ninguna característica adicional. 
41.	En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso. 

Paso	Descripción
42.	El proceso comenzará y una vez finalizado, y si todo ha ido bien bastará con pulsar sobre “Cerrar” para finalizar la desinstalación. 
43.	En caso de ser necesario el servidor requerirá un reinicio para finalizar la configuración. El “Administrador del servidor” mostrará una advertencia acerca de la necesidad de dicho reinicio. 

2.2. CONFIGURACIÓN GENERAL DE HYPER-V

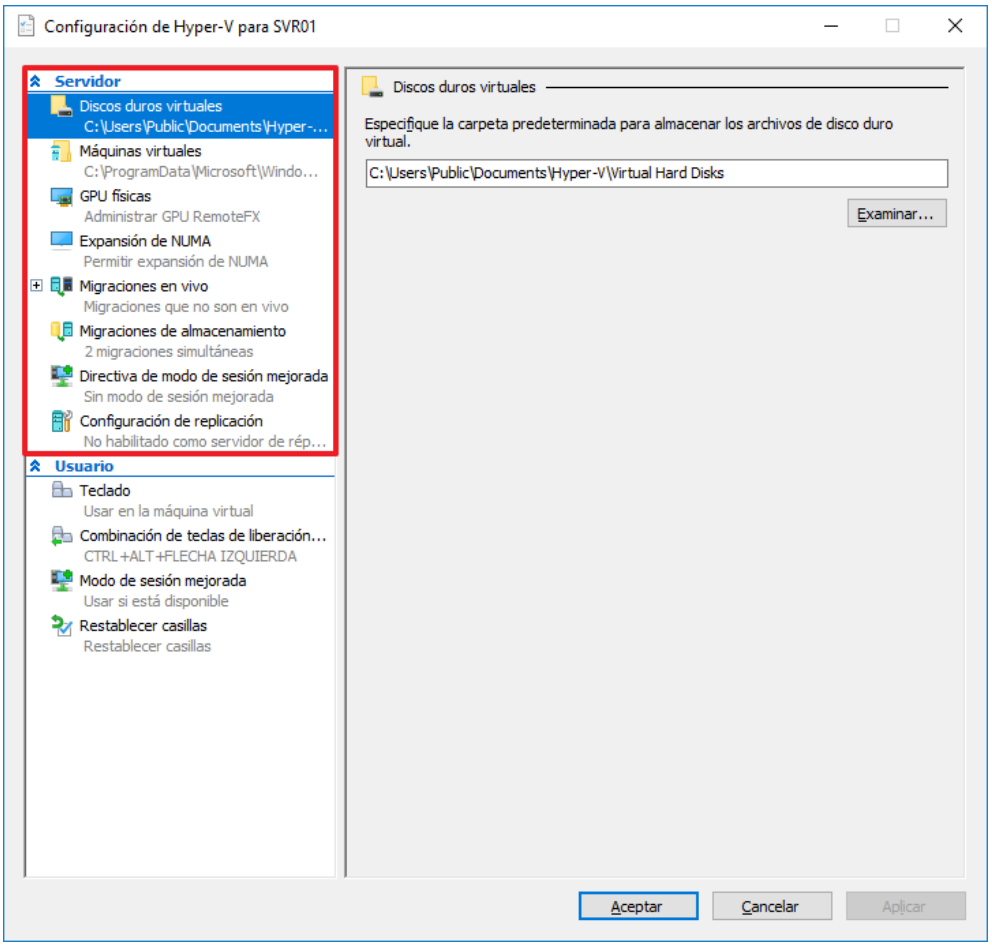
La gestión de la configuración de Hyper-V constituye una importante tarea de administración debido a que permite establecer o modificar configuraciones que afectan a la funcionalidad del servicio de virtualización

Paso	Descripción
44.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
45.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
46.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 

Paso	Descripción
47.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
48.	Dentro de la consola emergente seleccione el servidor de Hyper-V instalado en el servidor y a continuación en el panel de "Acciones" seleccione la opción "Configuración de Hyper-V…". 
49.	En los siguientes apartados se definirán las configuraciones dedicadas al propio servidor de Hyper-V y aquellas configuraciones que afectan a la experiencia de usuario con el servicio de virtualización.

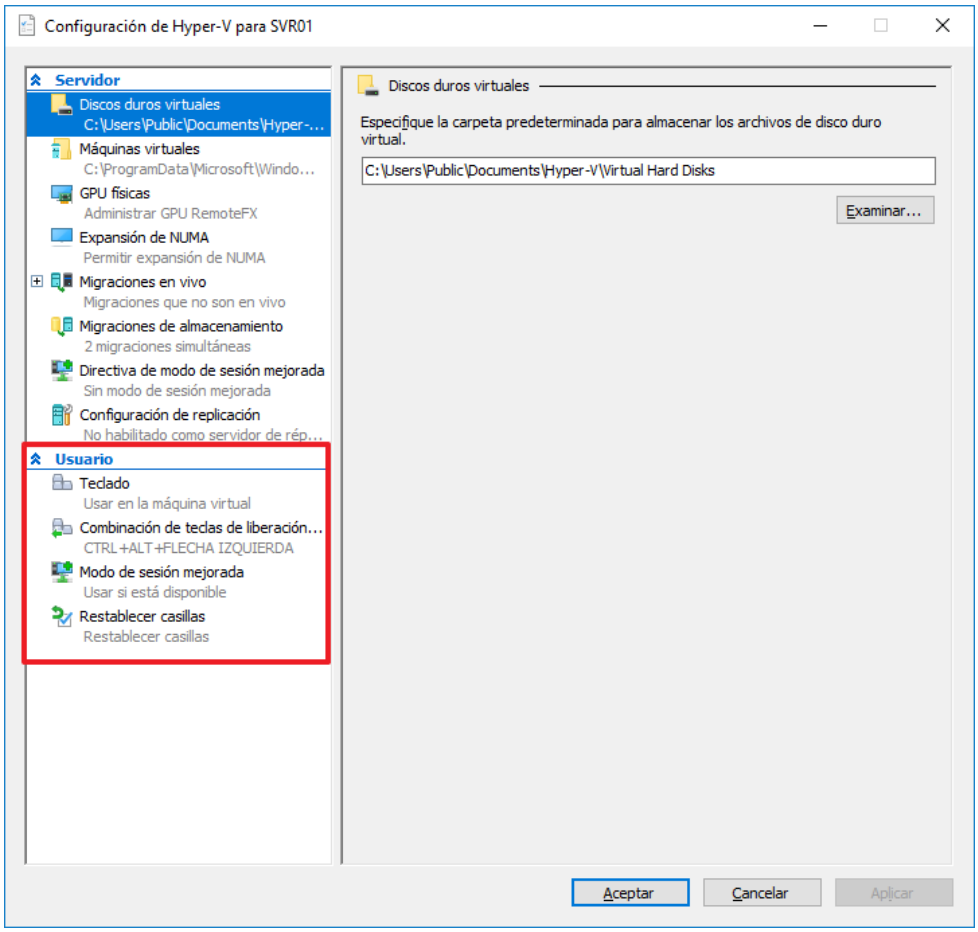
2.2.1. CONFIGURACIÓN DEL SERVIDOR

Este apartado define la configuración dedicada al servidor de Hyper-V la cual permite gestionar y administras las configuraciones más generales del servicio de virtualización.

Paso	Descripción
50.	Dentro de la ventana “Configuración de Hyper-V para <<su servidor>>” acceda al apartado denominado “Servidor”.
51.	Dentro de este apartado defina las configuraciones necesarias que permitan mejorar o establecer configuraciones de uso para el servidor Hyper-V. 
52.	Dentro de estas configuraciones que es posible deberá prestar especial atención a las siguientes: – **Discos duros virtuales:** permite definir la ubicación por defecto de los discos de las máquinas virtuales. – **Máquinas virtuales:** permite definir la ubicación por defecto de los ficheros que componen las máquinas virtuales. – **Migraciones en vivo:** permite realizar migraciones de máquinas virtuales mientras éstas se encuentran en uso. – **Configuración de replicación:** esta configuración permite disponer de una copia casi instantánea en otro servidor de Hyper-V.

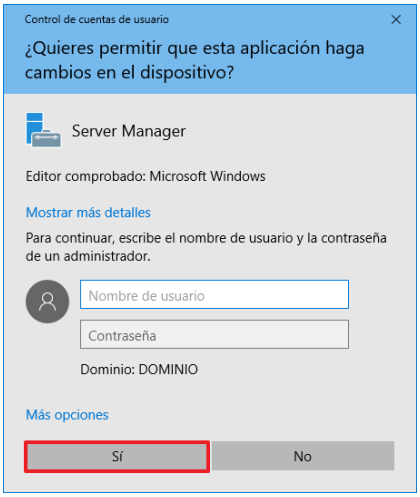
2.2.2. CONFIGURACIÓN DEL USUARIO

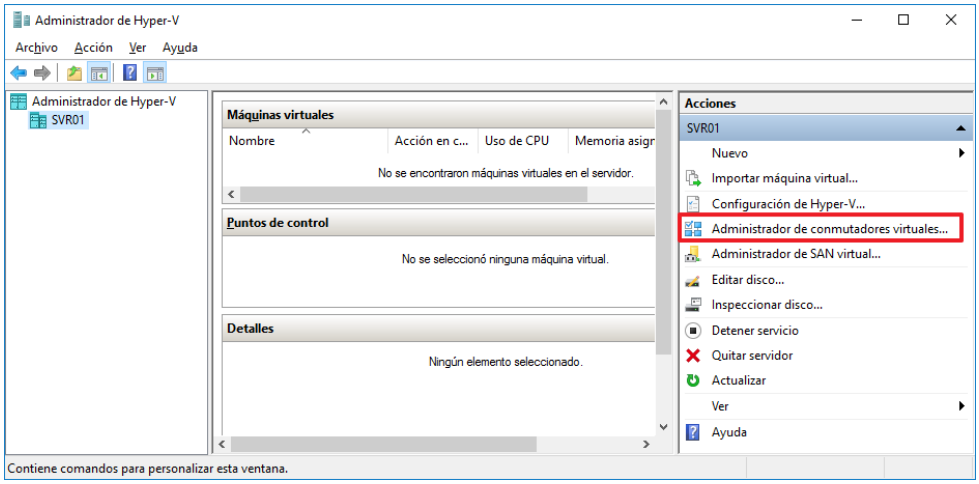
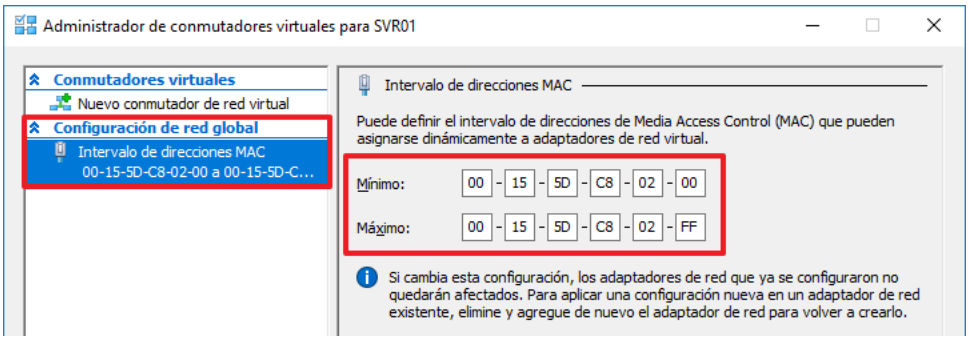
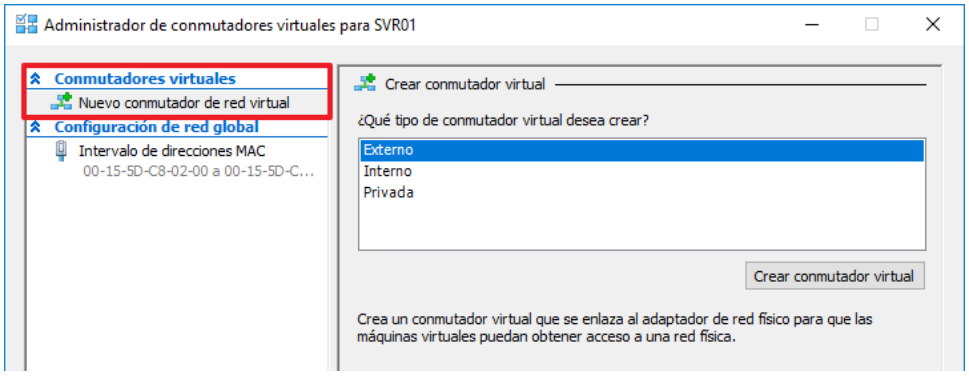
Este apartado define la configuración dedicada al usuario en su interacción con el servicio de virtualización.

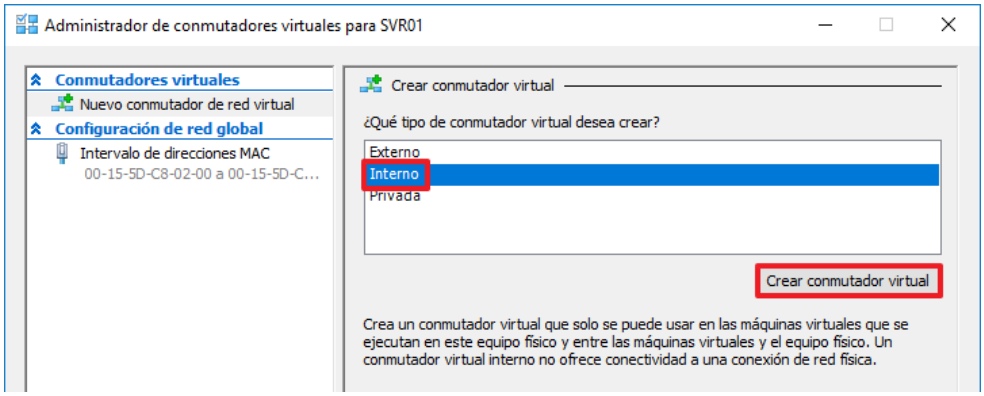
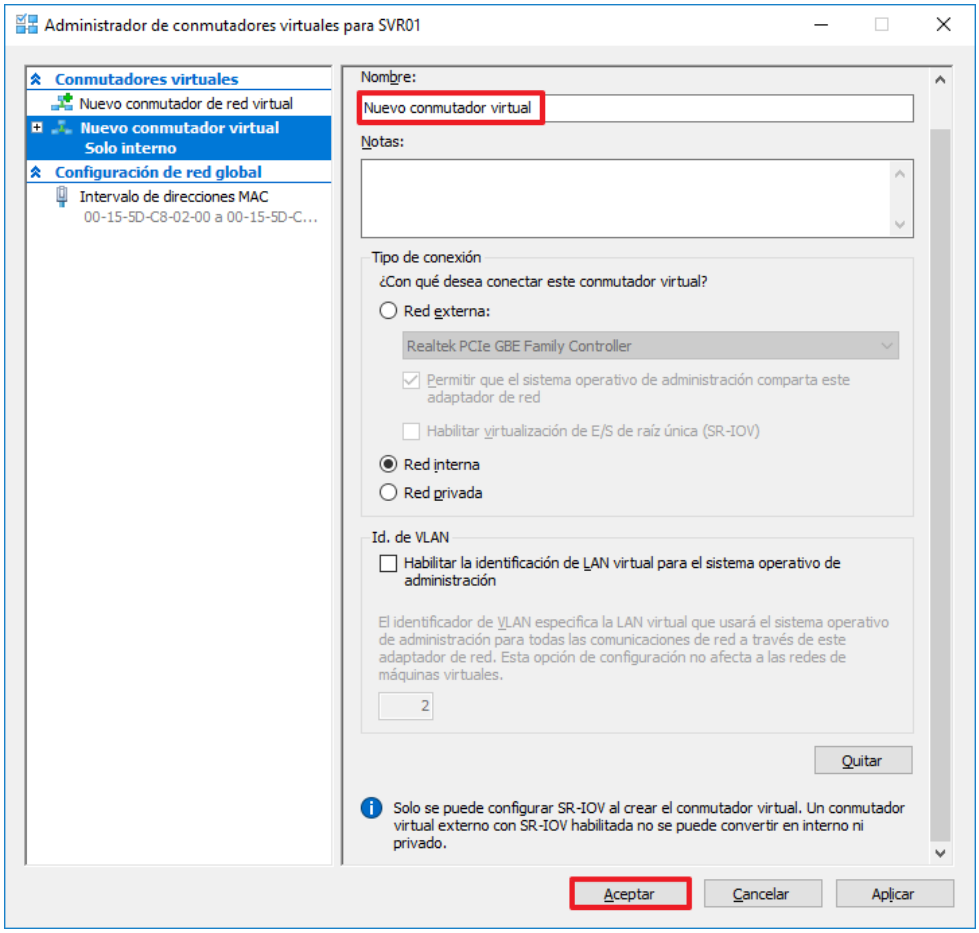
Paso	Descripción
53.	Dentro de la ventana “Configuración de Hyper-V para <<su servidor>>” acceda al apartado denominado “Usuario”.
54.	Dentro de este apartado defina las configuraciones necesarias que permitan mejorar o establecer configuraciones de uso para el servidor Hyper-V. 
55.	Las configuraciones de las que dispone este apartado son las siguientes: – **Teclado:** permite establecer cómo se comportan las combinaciones de teclado en las máquinas virtuales. – **Combinación de teclas de liberación del mouse:** define la combinación de teclas a utilizar para “liberar” el ratón de la máquina virtual sobre la que se está trabajando. – **Modo de sesión mejorada:** permite el redireccionamiento de dispositivos y recursos locales (copiar y pegar) de equipos que ejecutan una conexión con una máquina virtual. – **Reestablecer casillas:** permite volver a un estado de “recién instalado” en el que Hyper-V muestra mensajes de confirmación que han sido ya omitidos.

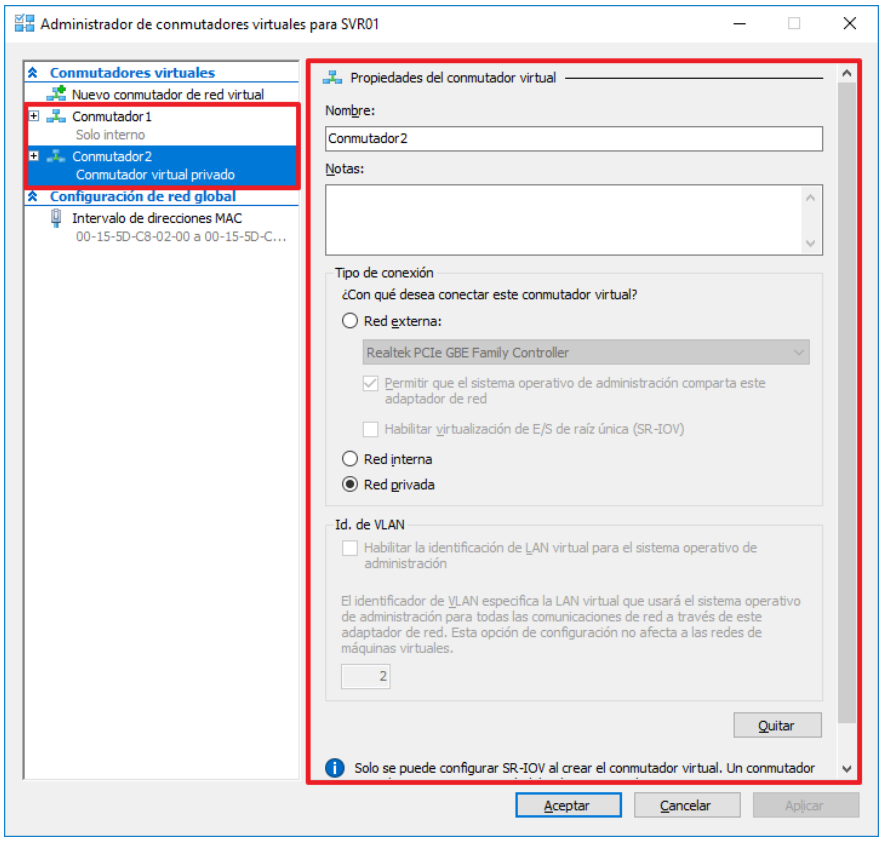
2.3. GESTIÓN DE CONMUTADORES VIRTUALES

Dentro del servidor de Hyper-V es importante realizar una correcta gestión de las redes disponibles con el fin de determinar cómo se comporta la red de las diferentes máquinas virtuales y permitir establecer o denegar comunicaciones según sea necesario.

Paso	Descripción
56.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
57.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas.
58.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí". 
59.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 

Paso	Descripción
60.	Dentro de la consola emergente seleccione el servidor de Hyper-V instalado en el servidor y a continuación en el panel de “Acciones” seleccione la opción “Administrador de conmutadores virtuales”. 
61.	En la ventana emergente “Administrador de conmutadores virtuales para <<su servidor>>” dentro del apartado “Configuración de red global” seleccione “Intervalo de direcciones MAC”. Establezca el intervalo mínimo y máximo de direcciones MAC que pueden asignarse a los adaptadores de red virtuales.  **Nota:** Deberá tener en cuenta las especificaciones necesarias para establecer el direccionamiento MAC adecuado. En este ejemplo, se establece por defecto.
62.	A continuación, seleccione dentro del apartado “Conmutadores virtuales” la opción “Nuevo conmutador de red virtual”. 

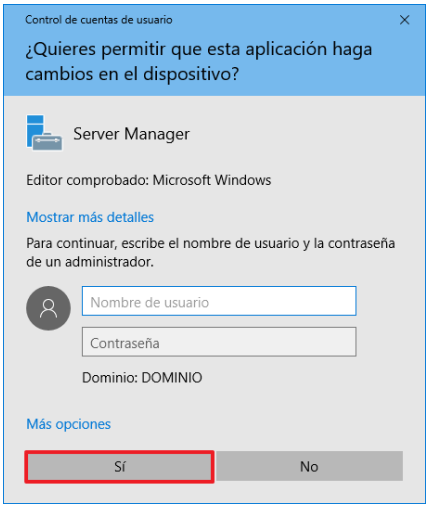
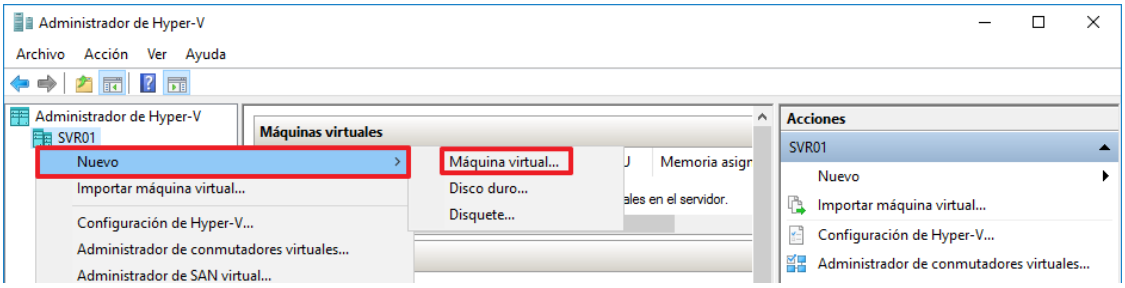
Paso	Descripción
63.	Seleccione entonces el tipo de conmutador virtual de red deseado. Deberá tener en consideración las necesidades de su organización en el momento de crear dichos adaptadores virtuales de red.  **Nota:** Para este ejemplo se crea un conmutador de red "Interno"
64.	Aparecerá otra ventana en la que se mostrarán las opciones disponibles sobre el adaptador de red creado. Establezca un nombre y si lo desea una descripción. Por último, pulse sobre "Aceptar". 

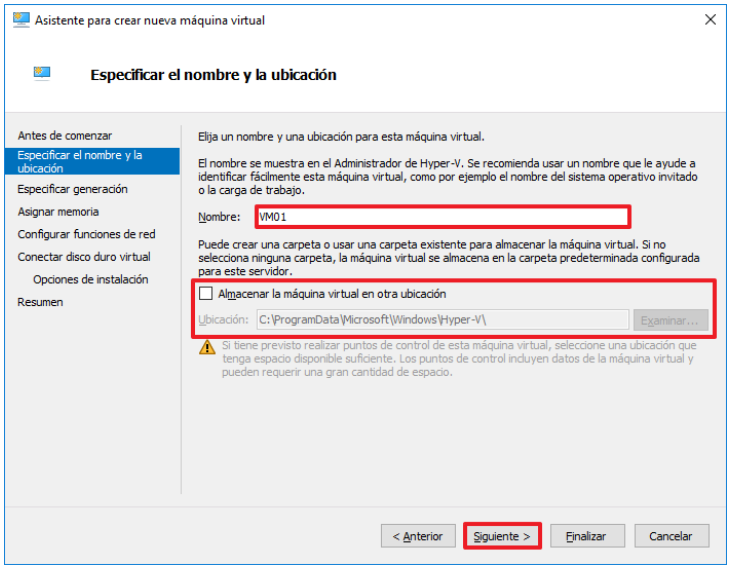
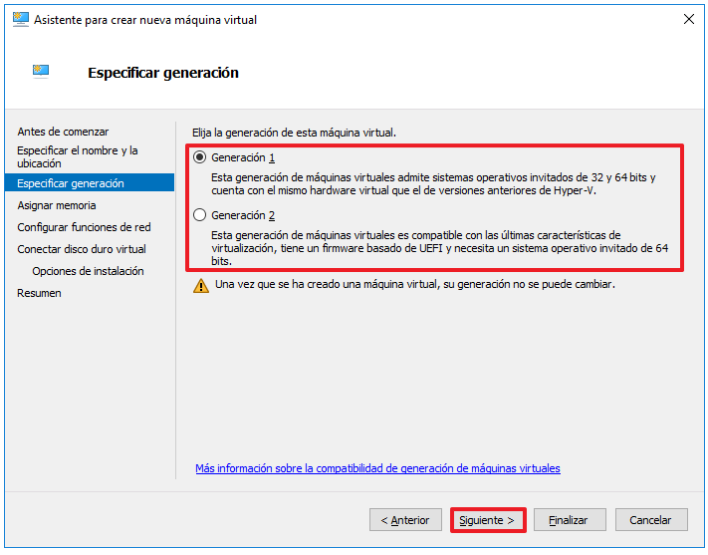
Paso	Descripción
65.	Podrá realizar una gestión sobre los conmutadores creados pulsando sobre cada uno de ellos y modificando la configuración que ya poseen. Del mismo modo es posible eliminar conmutadores que ya no sean requeridos haciendo uso del botón “Quitar”. 

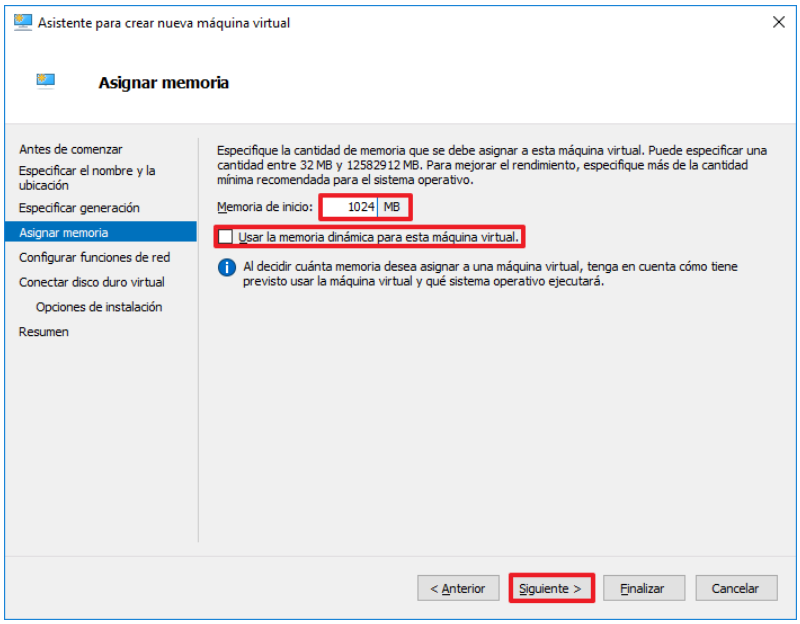
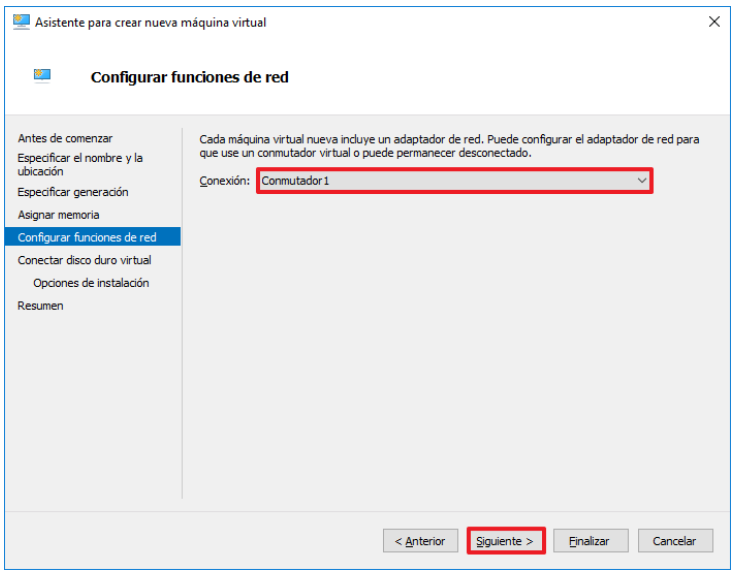
2.4. GESTIÓN DE MÁQUINAS VIRTUALES

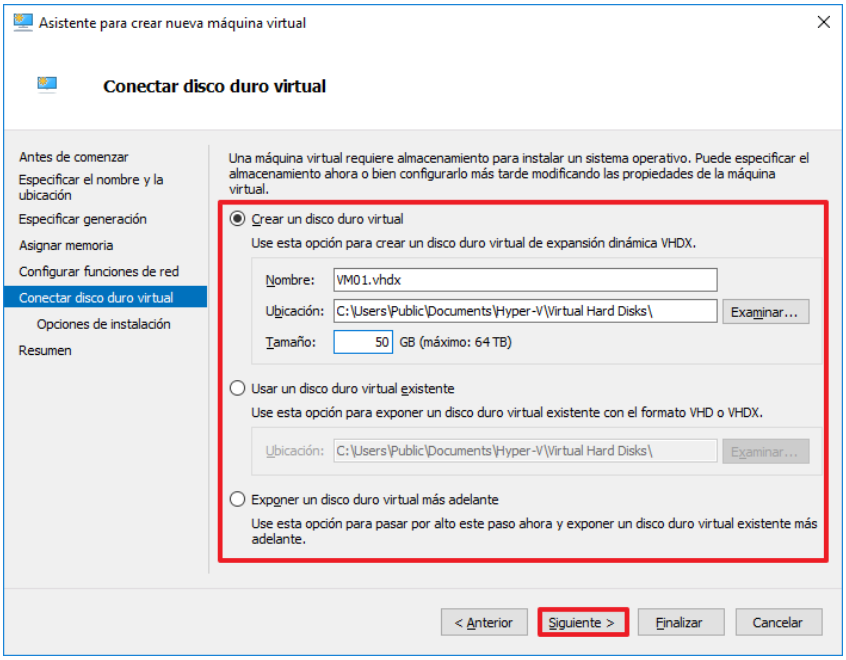
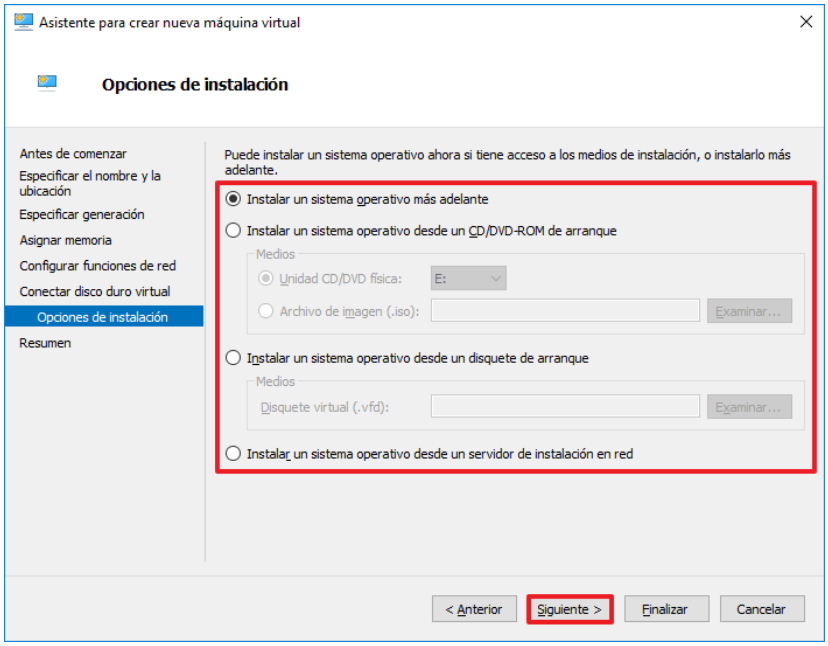
Otra de las tareas esenciales es la creación de máquinas virtuales ya que éstas son las que ofrecen el servicio propiamente dicho. En este apartado se realiza un ejemplo de creación y configuración de una máquina virtual.

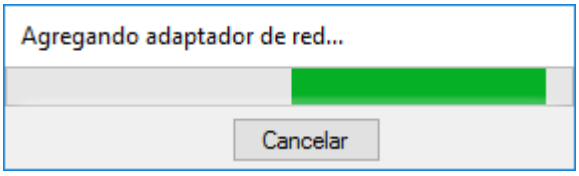
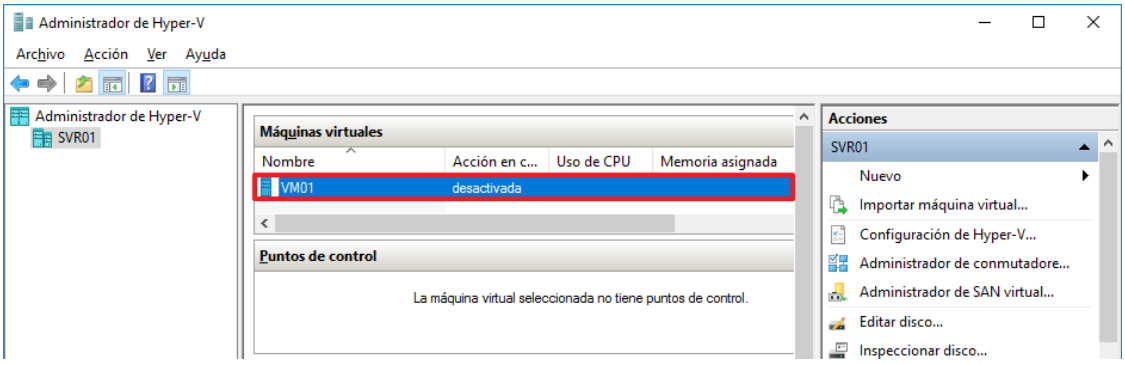
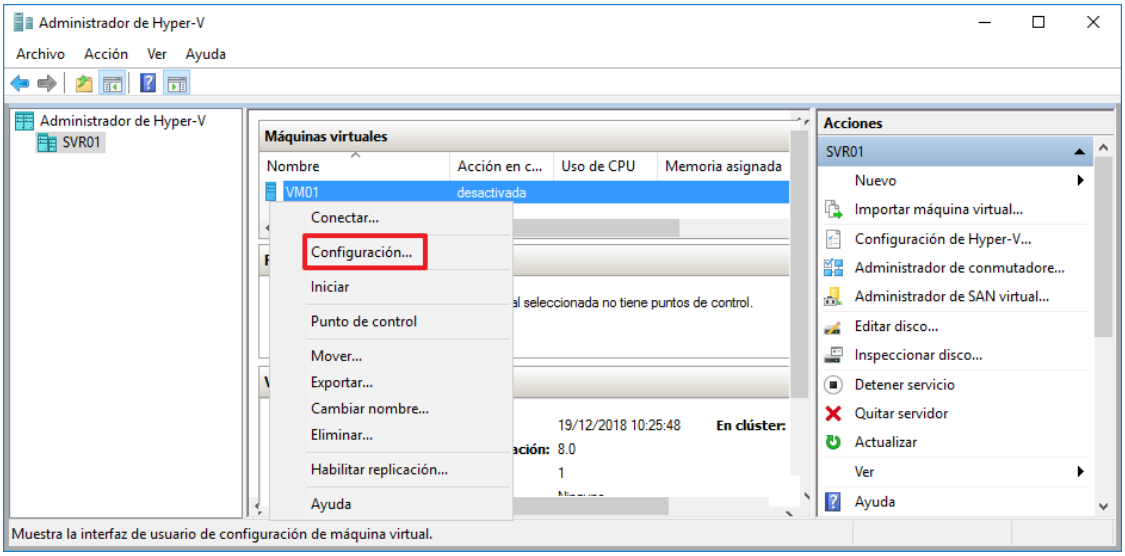
Paso	Descripción
66.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

Paso	Descripción
67.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
68.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
69.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
70.	Dentro de la consola emergente seleccione el servidor de Hyper-V con el botón derecho y seleccione la opción del menú contextual **"Nuevo → Máquina virtual…"**.  **Nota:** En este ejemplo el servidor de denomina "SVR01". Deberá adaptar estos pasos a las configuraciones de su organización.
71.	Aparecerá el asistente para la creación de máquinas virtuales. En la ventana "Antes de comenzar" pulse "Siguiente >".

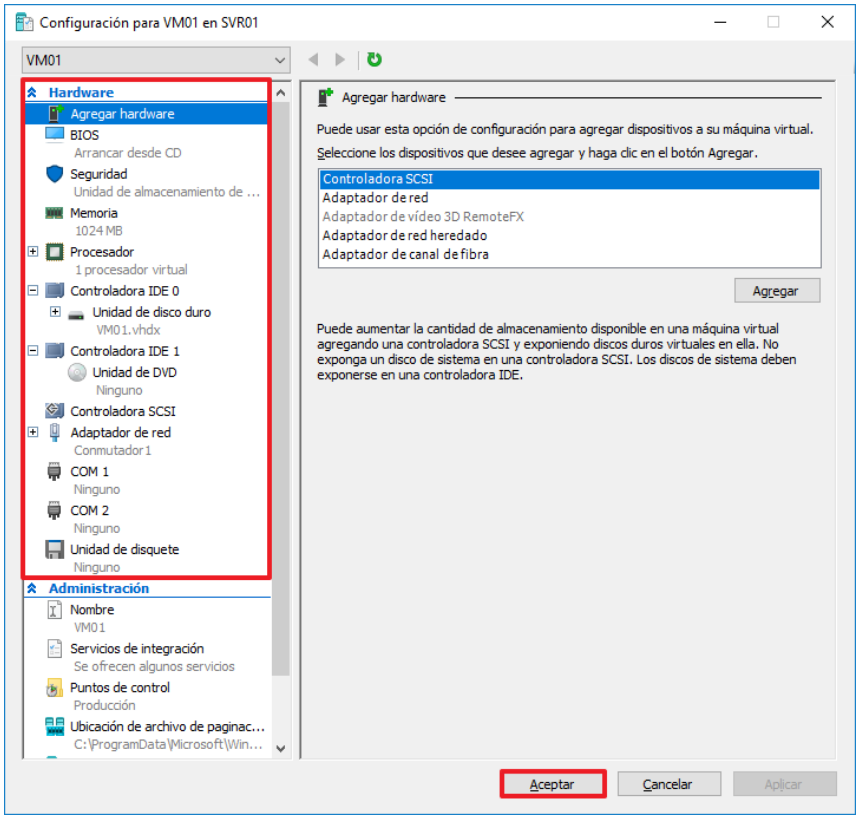
Paso	Descripción
72.	En la ventana “Especificar el nombre y la ubicación” determine el nombre que poseerá la máquina dentro de Hyper-V y una ubicación concreta si lo desea. Pulse “Siguiente >” para continuar.  **Nota:** Tenga en consideración que si realizó alguna modificación en el apartado “2.2 CONFIGURACIÓN GENERAL DE HYPER-V” la ubicación por defecto ya deberá estar configurada a la requerida por su organización. En este ejemplo se crea la máquina “VM01”, deberá adaptar los nombres a las necesidades de su organización”.
73.	En la ventana “Especificar generación” deberá determinar la generación de las máquinas creadas. Esto afectará en las características de las mismas. Pulse “Siguiente >” cuando haya finalizado.  **Nota:** En este ejemplo se opta por marcar “Generación 1”. Esta configuración deberá adaptarse a las necesidades de su organización. Una vez creada la máquina esta configuración no puede modificarse. Tenga este hecho presente de cara a futuras configuraciones que puedan ser requeridas como el “ANEXO A.5.2 CIFRADO DE MÁQUINAS VIRTUALES”.

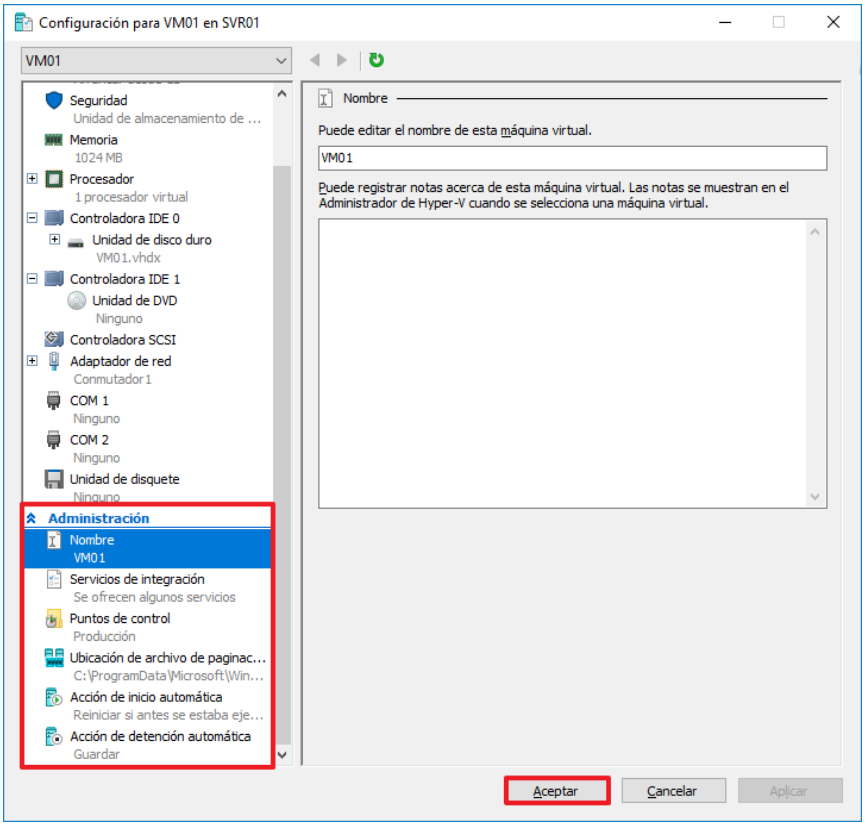
Paso	Descripción
74.	En la ventana “Asignar memoria” deberá determinar la memoria RAM de la máquina virtual. Además, podrá establecer el uso de memoria RAM de forma dinámica si lo desea. Pulse “Siguiente >” para seguir con el asistente.  **Nota:** Dependiendo de los recursos y las especificaciones de la máquina a implementar deberá configurar este valor. En este ejemplo se asigna “1024 MB” de memoria RAM.
75.	En la ventana “Configurar funciones de red” asigne uno de los conmutadores de los que disponga ya configurados. Pulse sobre el botón “Siguiente >” cuando finalice.  **Nota:** Deberá conectar el adaptador deseado en función de las necesidades de su organización. Esta configuración puede modificarse también tras crear la máquina. En este ejemplo se asigna el adaptador “Conmutador1”.

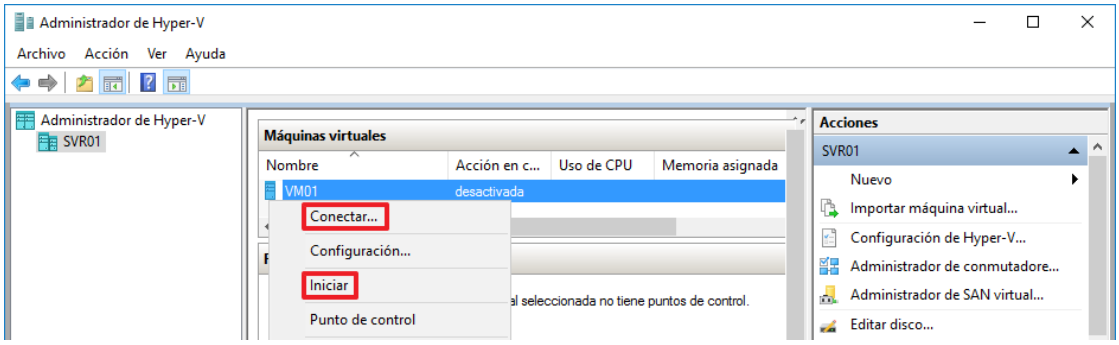
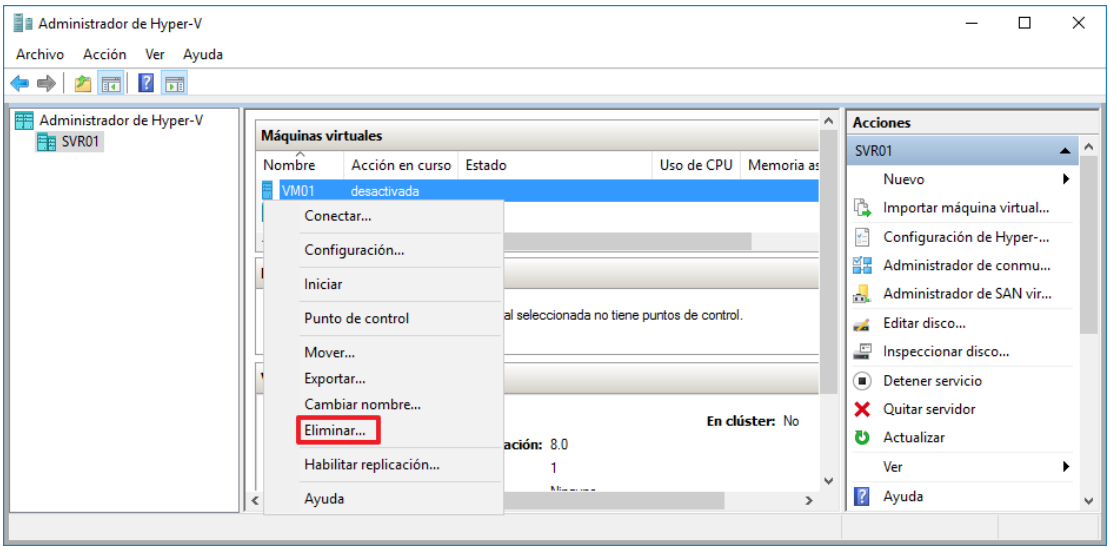
Paso	Descripción
76.	En la ventana “Conectar disco duro virtual” cree un disco duro virtual nuevo, asigne uno ya creado u omita este paso para exponer el disco más adelante. Pulse “Siguiente >” para continuar.  **Nota:** En este ejemplo se crea un disco virtual vacío con 50 GB de tamaño. Adapte el tamaño y la configuración a las necesidades de su organización.
77.	En la ventana “Opciones de instalación” configure un medio de arranque para la máquina virtual. Pulse “Siguiente >” cuando finalice.  **Nota:** En este ejemplo de opta por instalar un sistema operativo más adelante. Adapte este paso a las necesidades de su organización.

Paso	Descripción
78.	Por último, en la ventana “Resumen” compruebe que las configuraciones de la máquina virtual son correctas. En caso afirmativo pulse “Finalizar”. Si por el contrario requiere modificar alguna configuración pulse el botón “< Anterior” hasta llegar a la ventana deseada y modifique la configuración.
79.	Comenzará el proceso de creación el cual podrá variar dependiendo de las especificaciones de la máquina virtual. 
80.	Cuando haya finalizado la máquina virtual aparecerá en el panel central de “Administrador de Hyper-V”. 
81.	Para modificar la configuración establecida durante la creación o bien añadir más recursos haga clic derecho sobre la máquina deseada y pulse sobre la opción del menú contextual “Configuración…”. 

Paso	Descripción
82.	De mismo modo podrá realizar diferentes configuraciones que afectan al comportamiento de la máquina virtual y a la experiencia de usuario con dicha máquina. Pulse “Aceptar” cuando haya finalizado.

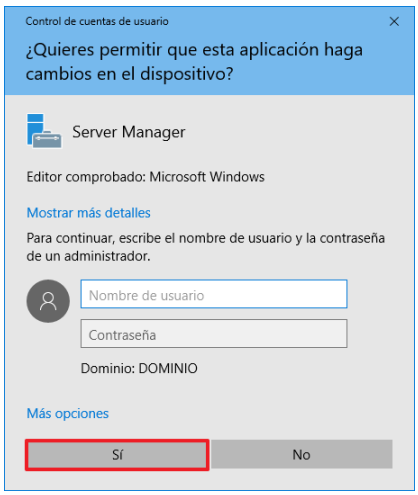


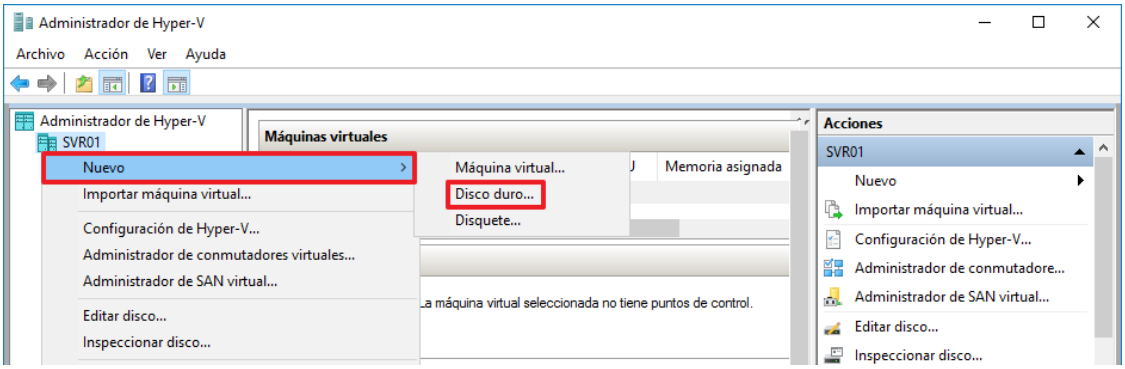
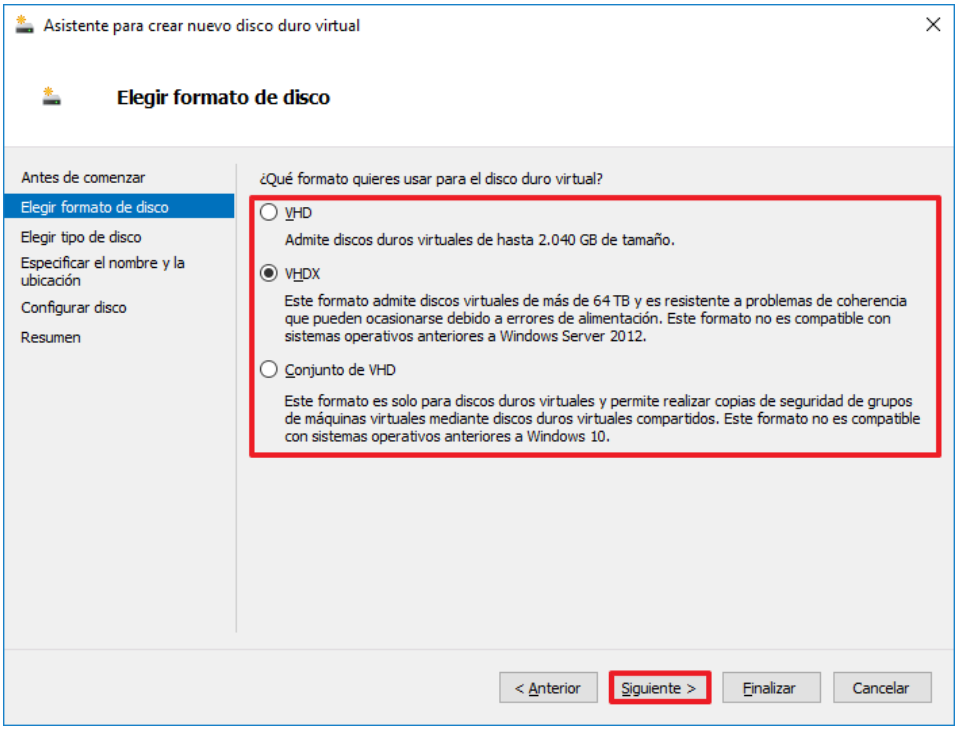


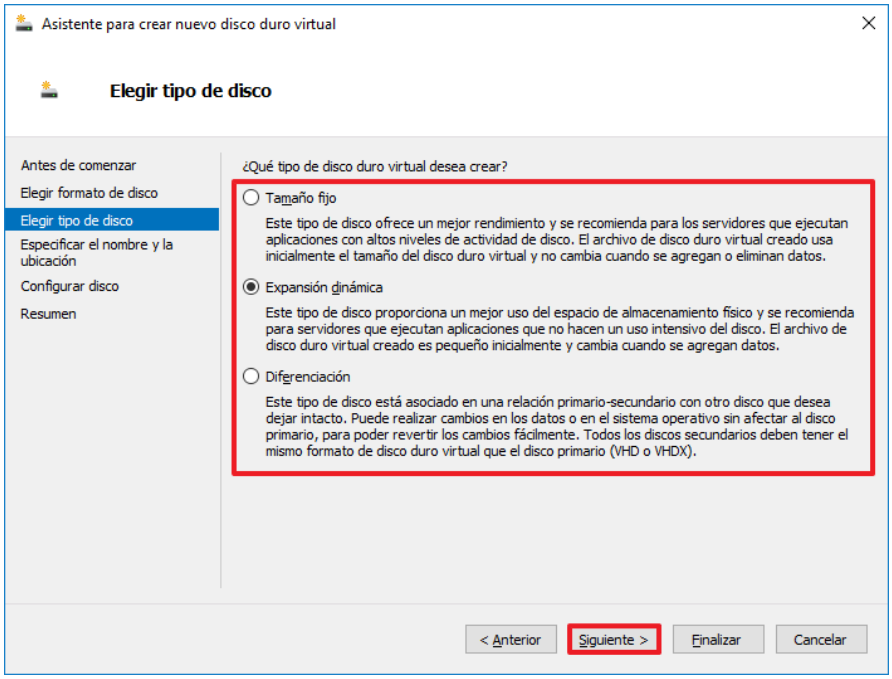
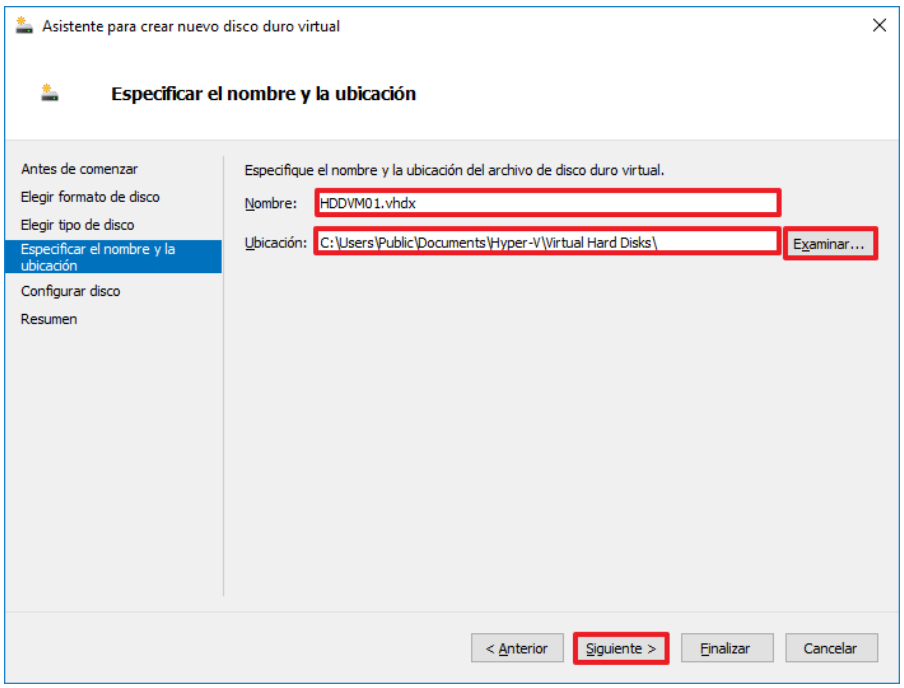
Paso	Descripción
83.	Por último, cuando la máquina esté finalizada podrá iniciarla y conectar con ella haciendo clic derecho y pulsando sobre las opciones del menú contextual “Iniciar” y “Conectar”, respectivamente. 
84.	En el caso de no disponer de disco virtual deberá consultar el apartado siguiente “2.5 GESTIÓN DE DISCOS DUROS VIRTUALES”.
85.	Si desea eliminar alguna de las máquinas haga clic derecho sobre ella y seleccione la opción del menú contextual “Eliminar…”.  **Nota:** Tenga en consideración que la eliminación de los discos asociados a la máquina deberá realizarse de forma manual.

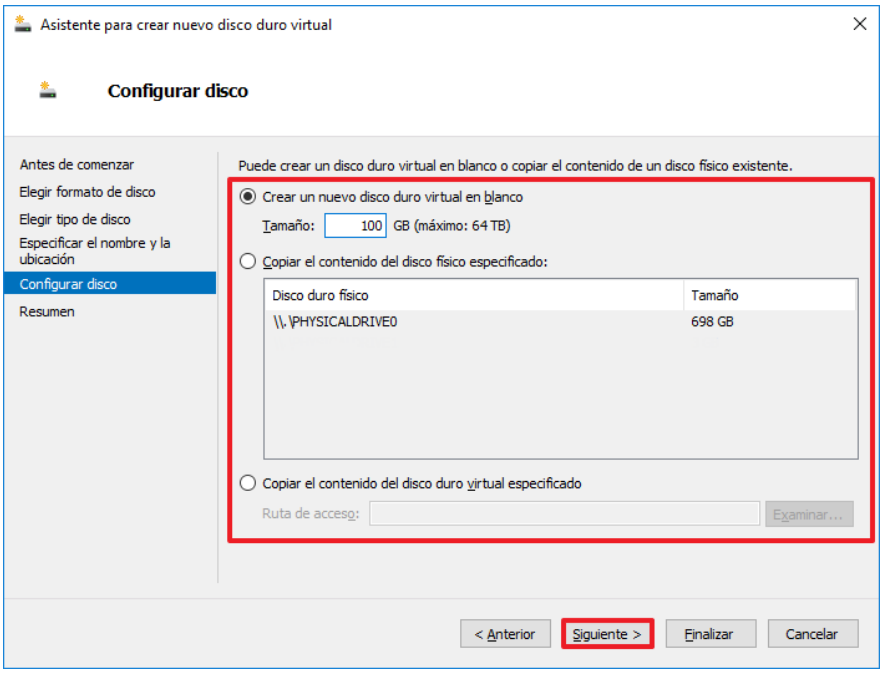
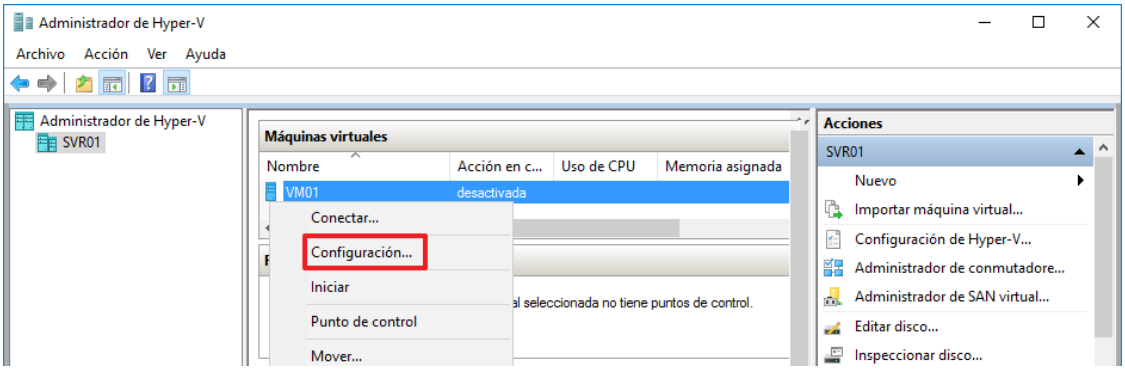
2.5. GESTIÓN DE DISCOS DUROS VIRTUALES

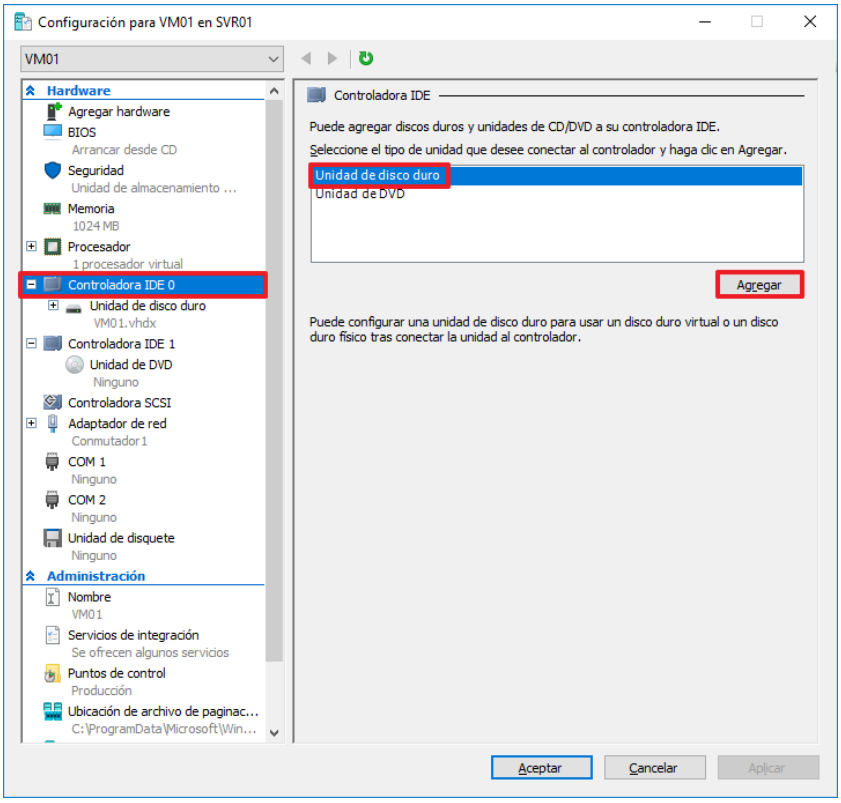
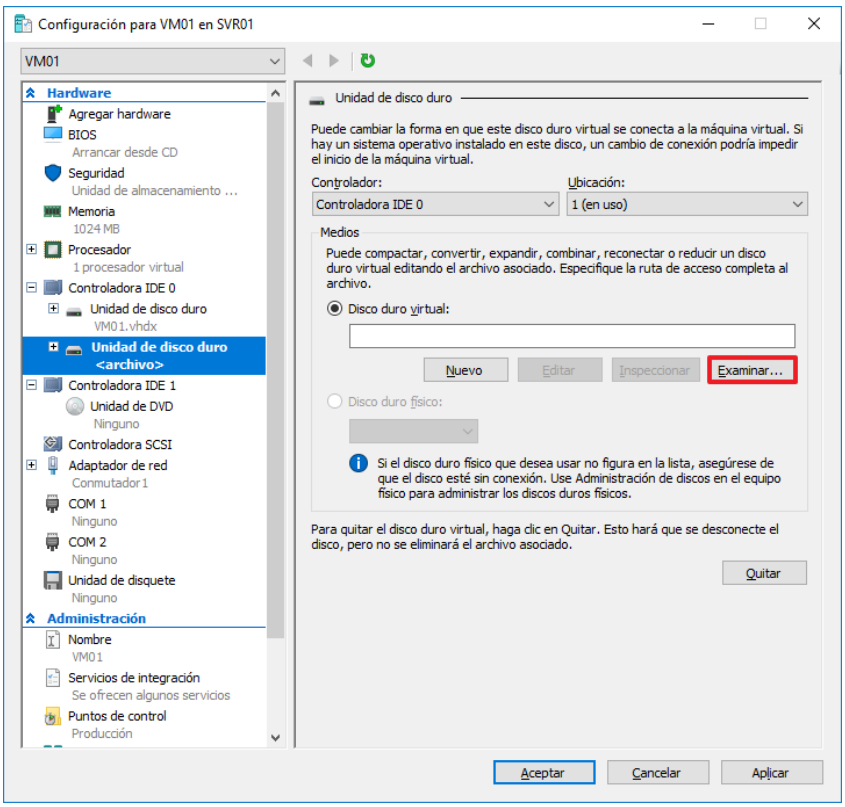
Los discos virtuales son el componente sobre el que se apoyan las máquinas virtuales para almacenar los recursos que se generan al igual que sucede en un equipo real. Este apartado define un ejemplo para crear un disco virtual que pueda ser utilizado con diferentes fines, bien como disco principal de una máquina o como disco adicional.

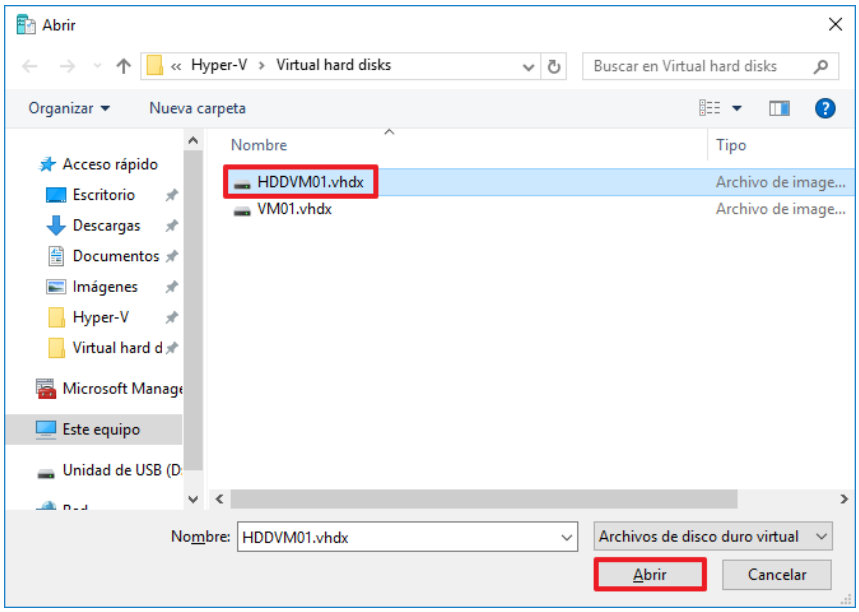
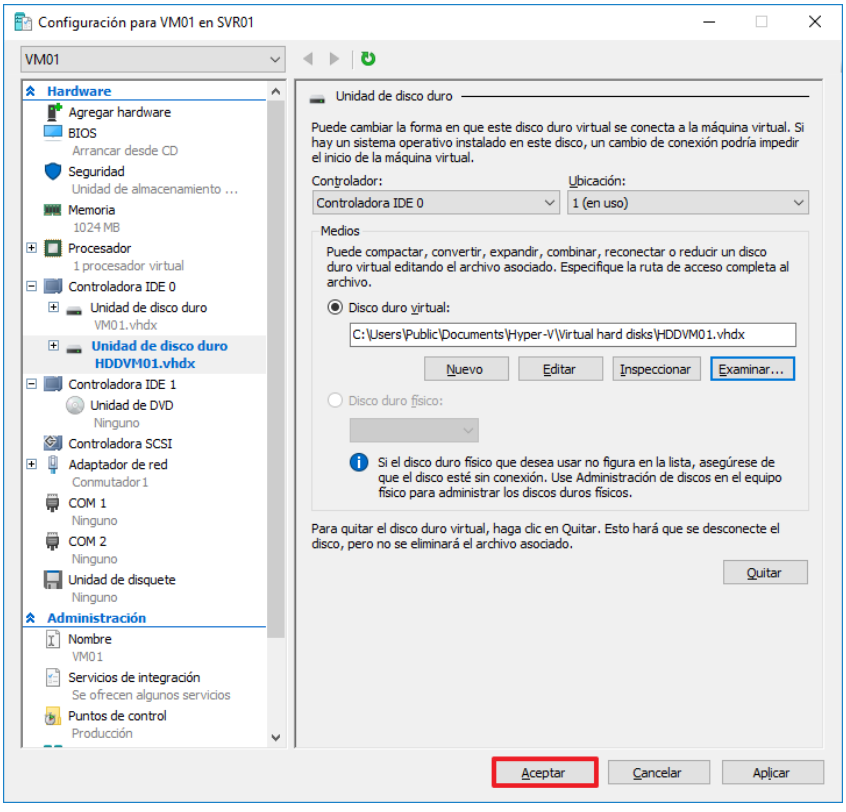
Paso	Descripción
86.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
87.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas.
88.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí". 
89.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 

Paso	Descripción
90.	Dentro de la consola emergente seleccione el servidor de Hyper-V con el botón derecho y seleccione la opción del menú contextual **"Nuevo → Disco duro…"**.  **Nota:** En este ejemplo el servidor de denomina "SVR01". Deberá adaptar estos pasos a las configuraciones de su organización.
91.	Aparecerá el asistente para la creación de discos virtuales. En la ventana "Antes de comenzar" pulse "Siguiente >".
92.	En la ventana "Elegir el formato de disco" deberá determinar el formato del disco dependiendo de las necesidades de su organización y de las máquinas virtuales que disponga. Pulse el botón "Siguiente >" para continuar.  **Nota:** En este ejemplo se crea un disco con formato "VHDX".

Paso	Descripción
93.	En la ventana “Elegir tipo de disco” deberá seleccionar como se dimensiona el disco cuando este almacena datos. Pulse “Siguiente >” cuando haya finalizado.  **Nota:** En este ejemplo se opta por una “Expansión dinámica” del disco.
94.	En la ventana “Especificar el nombre y ubicación” determine el nombre asociado al disco virtual y donde va a ser almacenado. Pulse “Siguiente >” para continuar.  **Nota:** Tenga en consideración que si realizó alguna modificación en el apartado “2.2 CONFIGURACIÓN GENERAL DE HYPER-V” la ubicación por defecto ya deberá estar configurada a la requerida por su organización. En este ejemplo se asigna el nombre “HDDVM01”.

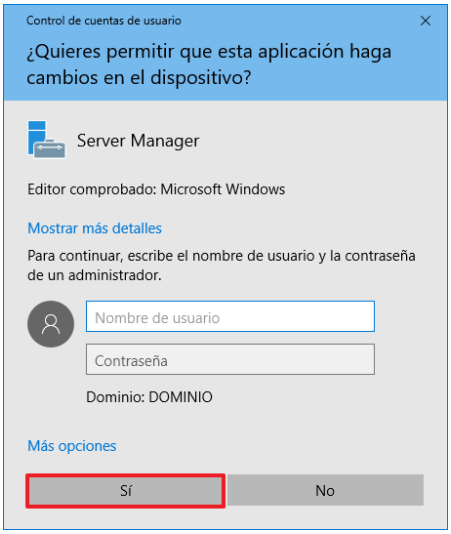
Paso	Descripción
95.	En la ventana “Configurar disco” deberá determinar las necesidades del disco duro creado pudiendo crear un disco en blanco (sin datos) o con datos copiados de otro disco existente. Pulse “Siguiente >” para continuar con el asistente.  **Nota:** En este ejemplo se genera un disco de 100 GB en blanco para asociarlo a una máquina virtual existente.
96.	Por último, en la ventana “Resumen” compruebe que las configuraciones del disco son correctas. En caso afirmativo pulse “Finalizar”. Si por el contrario requiere modificar alguna configuración pulse el botón “< Anterior” hasta llegar a la ventana deseada y modifique la configuración.
97.	Para asignar el disco recién creado seleccione la máquina afectada con el botón derecho y pulse sobre la opción del menú contextual “Configuración…”.  **Nota:** En este ejemplo se hace uso de la máquina virtual “VM01”. Adapte este y los siguientes pasos a las necesidades de su organización. La máquina virtual deberá estar apagada para realizar los siguientes pasos.

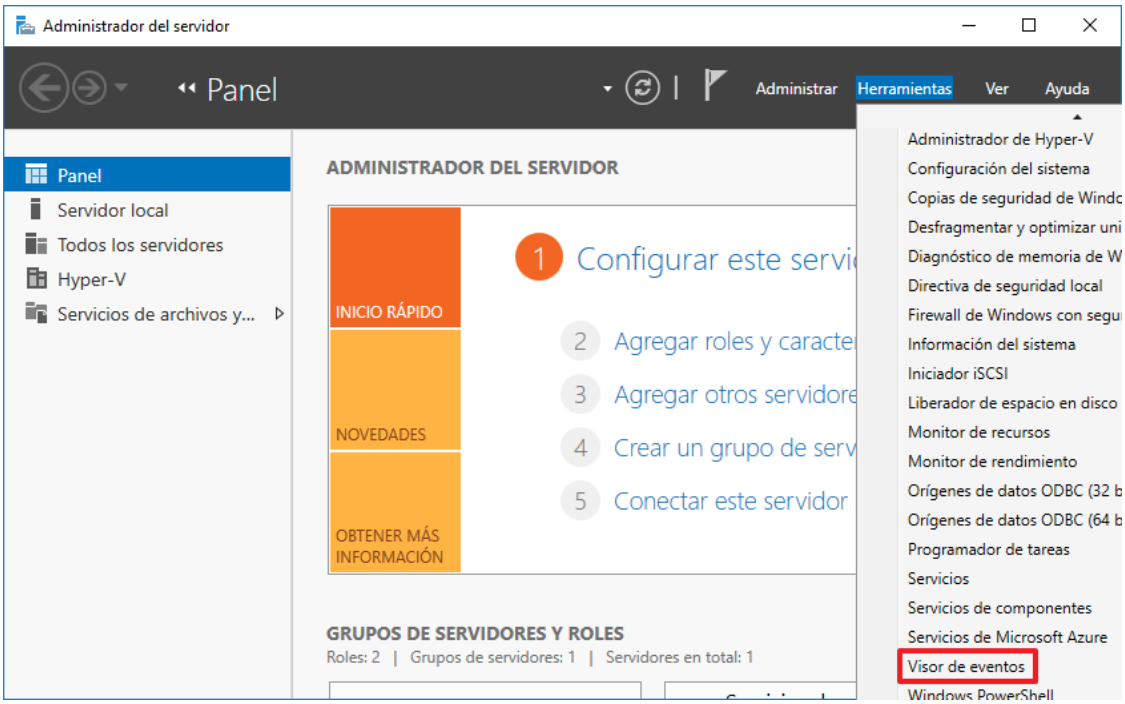
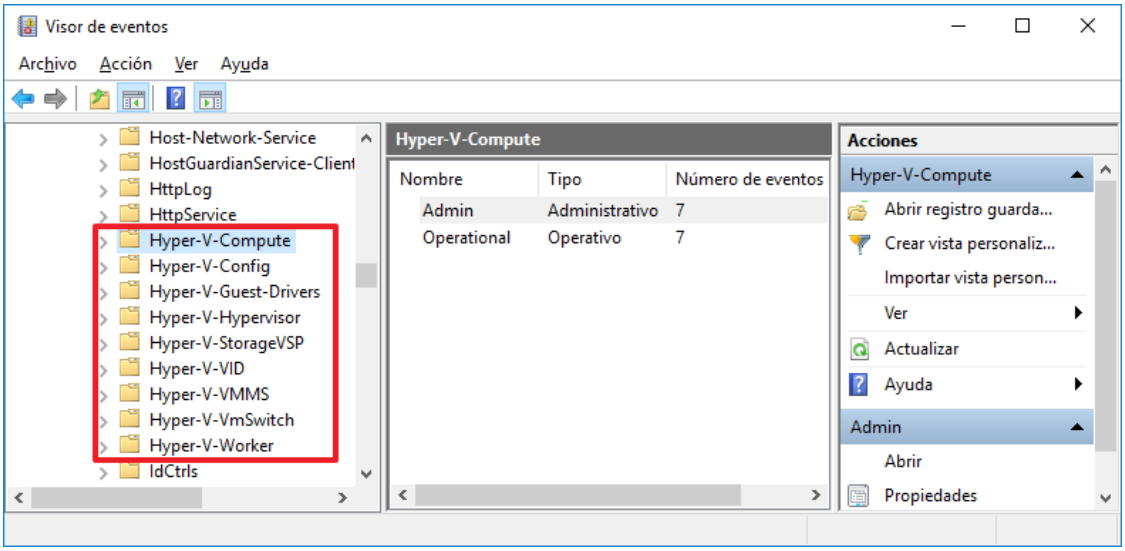
Paso	Descripción
98.	Sitúese sobre el apartado “Controladora IDE 0” y en el panel derecho seleccione “Unidad de disco duro”. Pulse sobre “Agregar” para continuar. 
99.	De nuevo en el panel derecho seleccione el botón “Examinar”. 

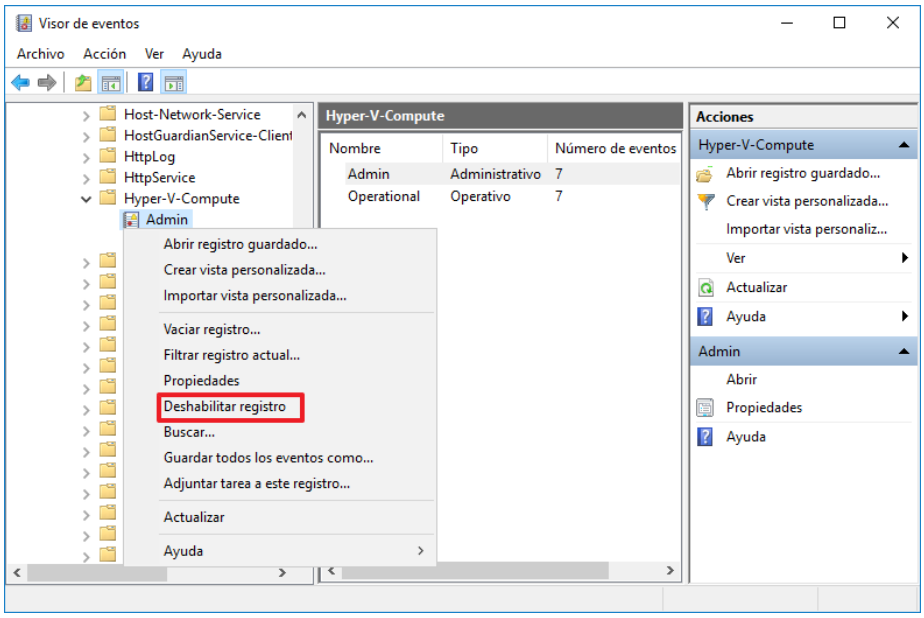
Paso	Descripción
100.	Ubíquese sobre la ruta en la que se creó el disco duro virtual, selecciónelo y pulse el botón “Abrir”. 
101.	Por último, pulse “Aceptar” para guardar los cambios. A partir de este momento la máquina virtual estará en posesión de un disco duro adicional. 

2.6. REGISTRO DE EVENTOS EN HYPER-V

Todos los eventos que se suceden en el servidor de Hyper-V deben ser recogidos por el equipo con el fin de determinar las acciones realizadas sobre el propio servidor y sobre las máquinas que este alberga.

Paso	Descripción
102.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
103.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
104.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 

Paso	Descripción
105.	Inicie la herramienta “Visor de eventos”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Visor de eventos”**. 
106.	En consola “Visor de eventos” despliegue el nodo **“Visor de eventos (local) → Registro de aplicaciones y servicios → Microsoft → Windows”**. En el listado de carpetas sitúese sobre aquellas que hagan referencia a Hyper-V.  **Nota:** Puede obtener más información acerca de los eventos registrados por Hyper-V en el siguiente enlace: https://blogs.technet.microsoft.com/virtualization/2018/01/23/looking-at-the-hyper-v-event-log-january-2018-edition/

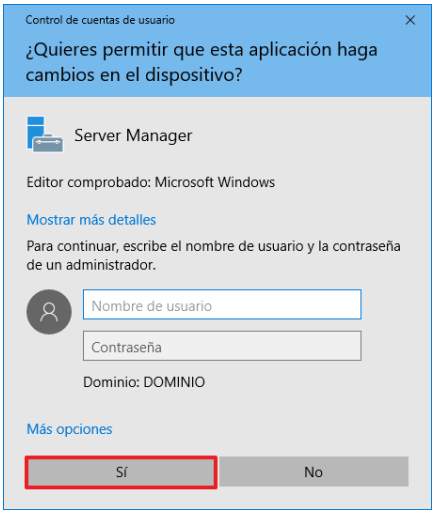
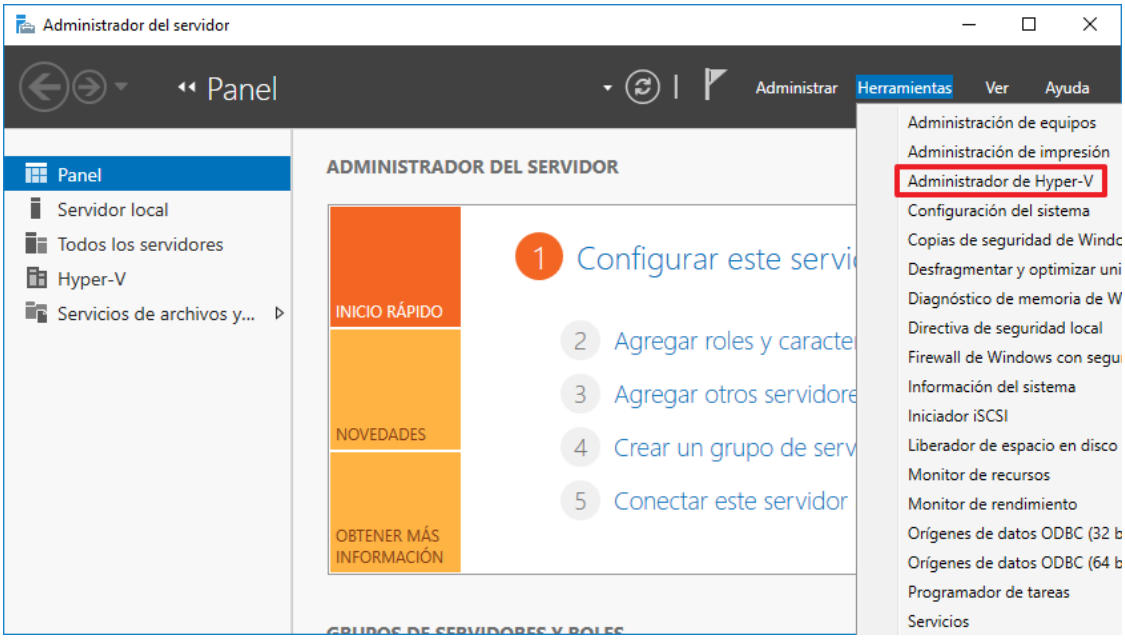
Paso	Descripción
107.	Por último, asegúrese que dentro de cada directorio se encuentra activado el registro haciendo clic derecho sobre cada uno de los elementos. En el caso de que el registro este habilitado aparecerá la opción “Deshabilitar registro”. Si por el contrario no se encuentra habilitado el registro aparecerá la opción “Habilitar registro”. 

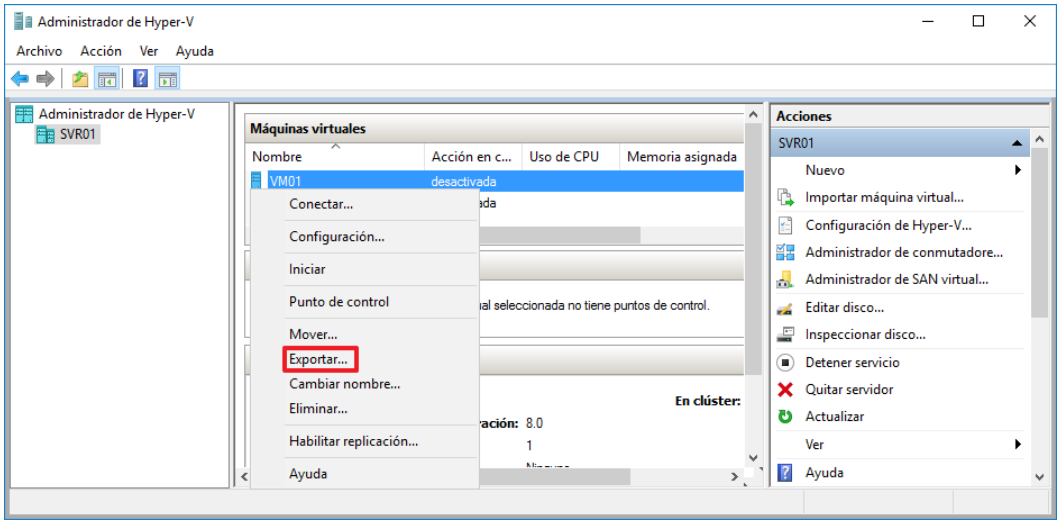
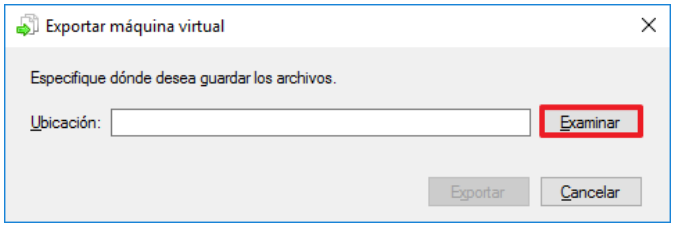
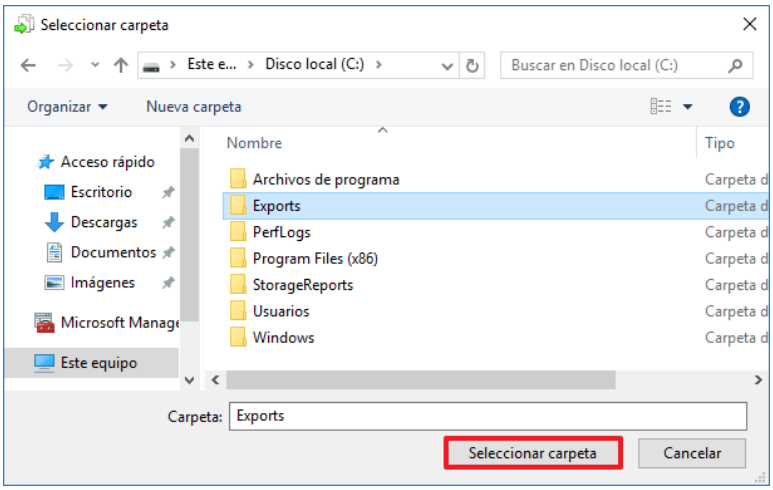
2.7. COPIAS DE SEGURIDAD DE MÁQUINAS VIRTUALES

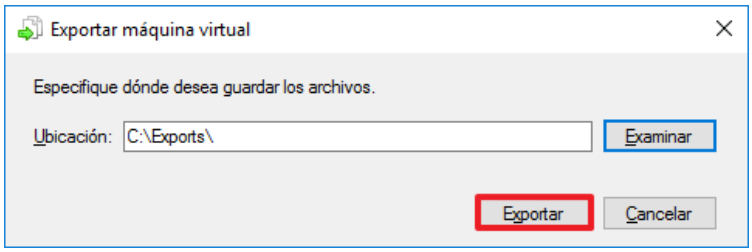
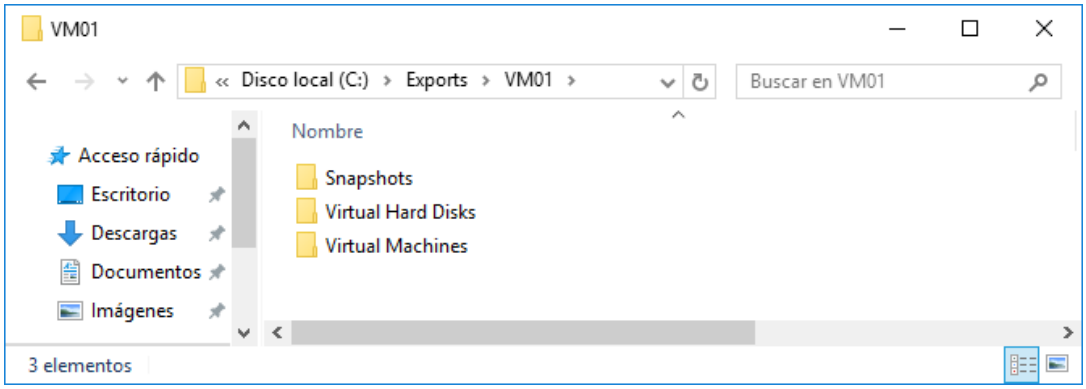
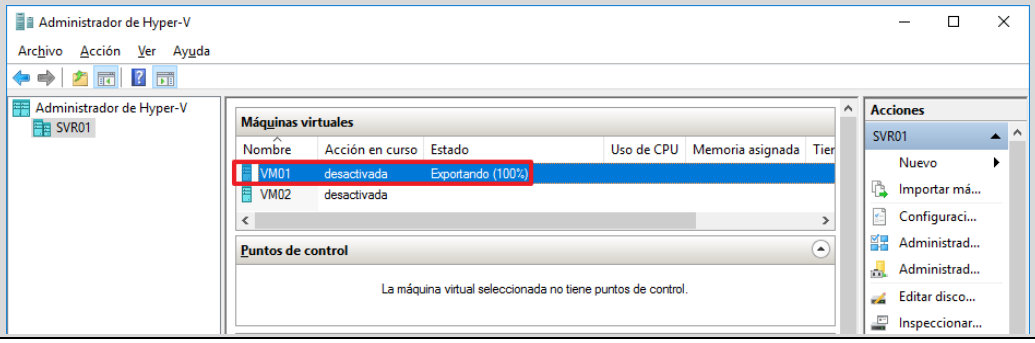
Hyper-V dispone de varias opciones para realizar copias de seguridad de las máquinas con el objetivo de mantener la continuidad y evitar la pérdida de datos. Aunque tal y como se explicó en apartados anteriores es posible configurar un servidor como equipo de réplicas se va a optar por una opción que permite realizar copias si no se dispone de un servidor adicional.

2.7.1. EXPORTAR MÁQUINAS VIRTUALES

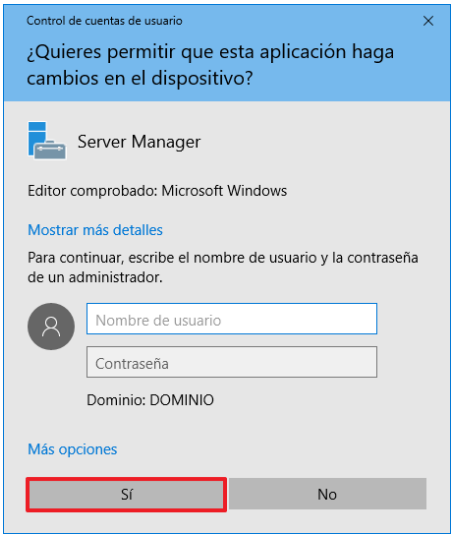
Paso	Descripción
108.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

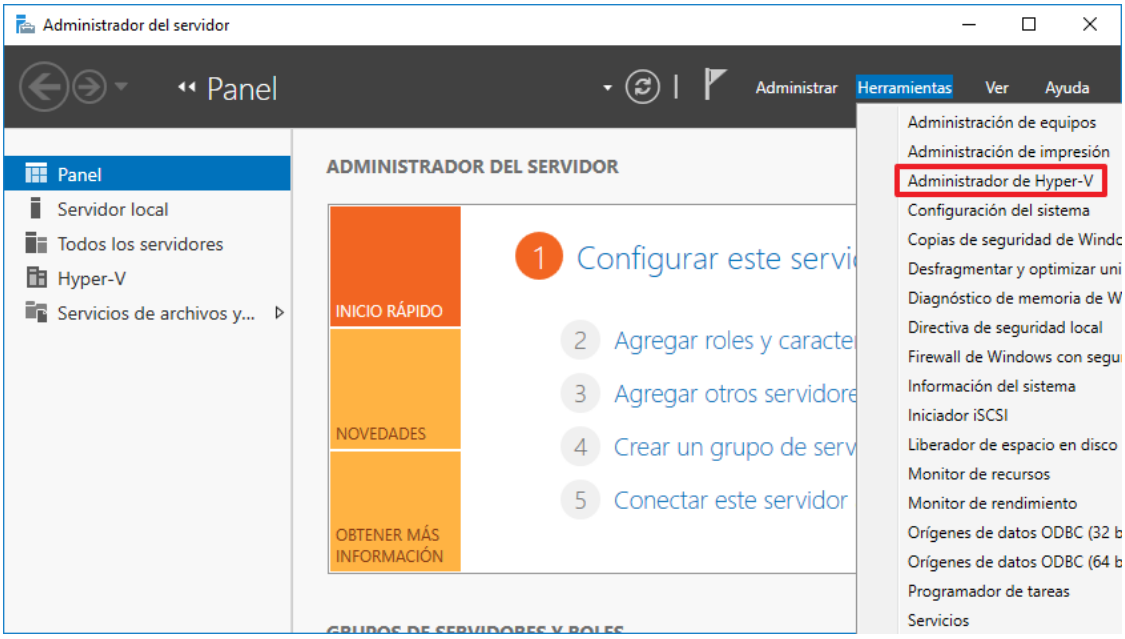
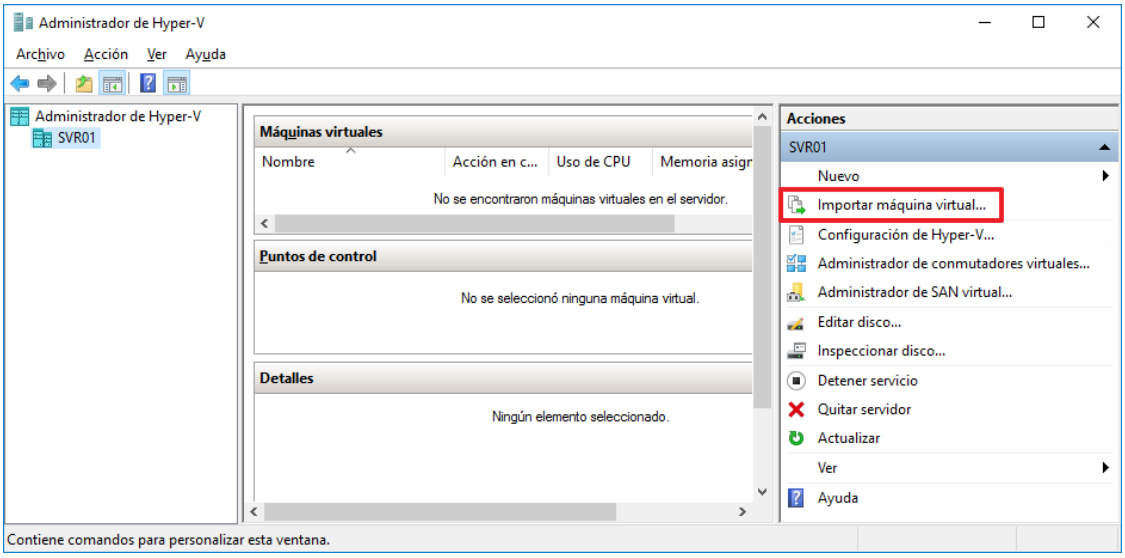
Paso	Descripción
109.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
110.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
111.	Inicie la herramienta “Administrador de Hyper-V”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administrador de Hyper-V”**. 

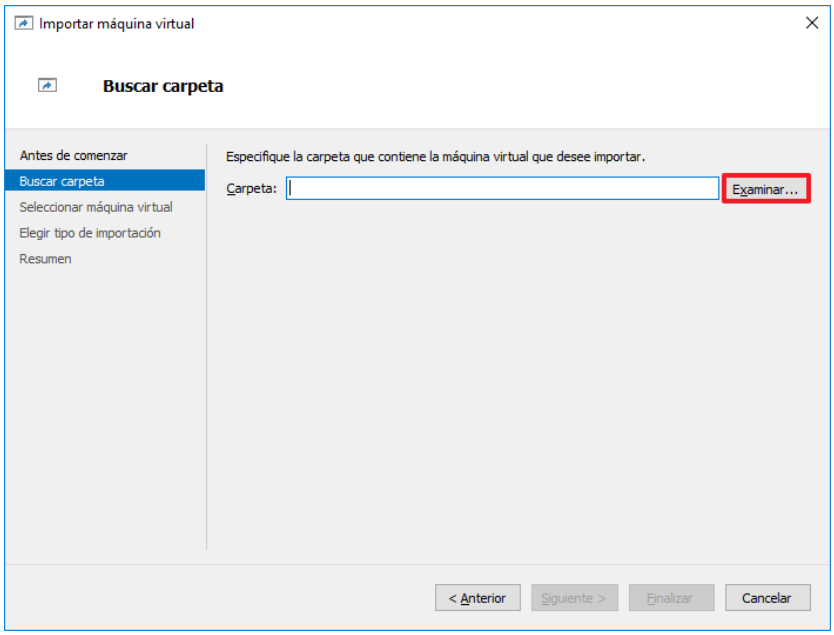
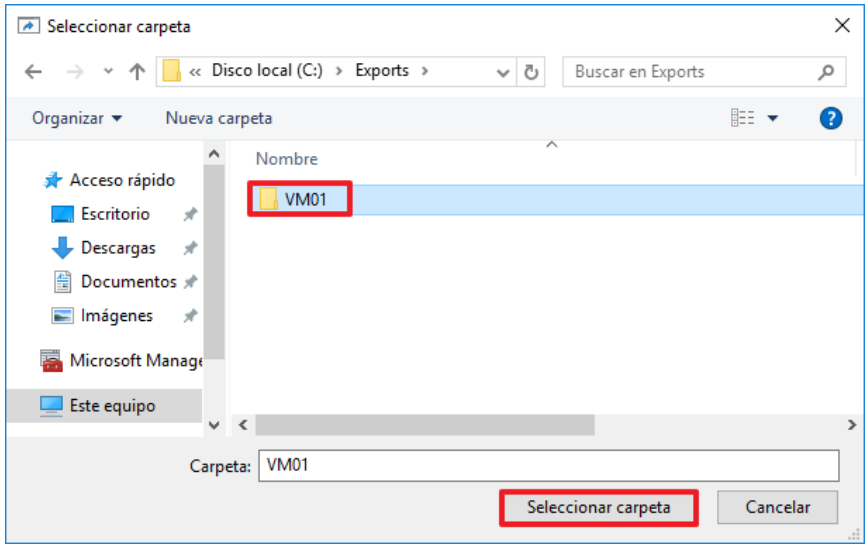
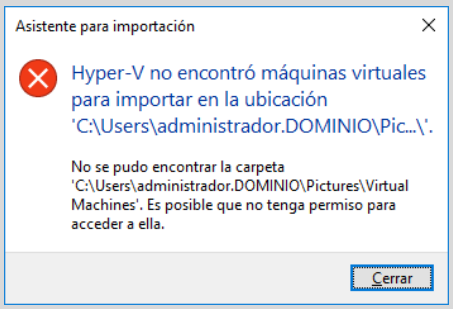
Paso	Descripción
112.	Seleccione la máquina virtual sobre la que desea realizar una copia de seguridad y pulse sobre la opción “Exportar…”.  **Nota:** En este ejemplo se realiza la exportación de la máquina “VM01”.
113.	En la ventana emergente pulse sobre el botón “Examinar”. 
114.	Seleccione la ubicación sobre la que desea exportar la máquina y pulse sobre el botón “Seleccionar carpeta”.  **Nota:** En este ejemplo se utiliza el directorio “Exports” ubicado en “C:\”.

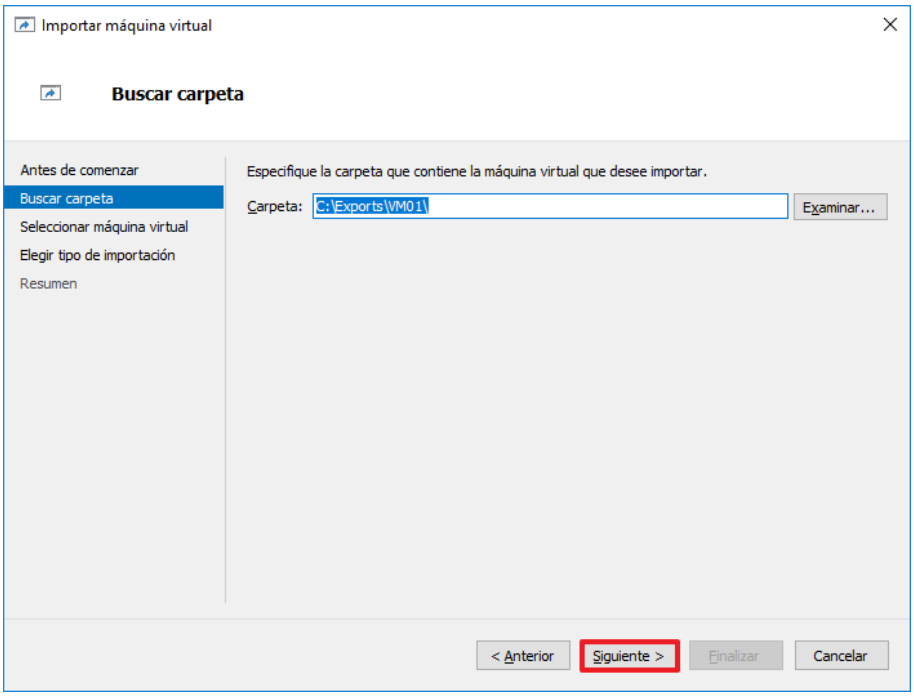
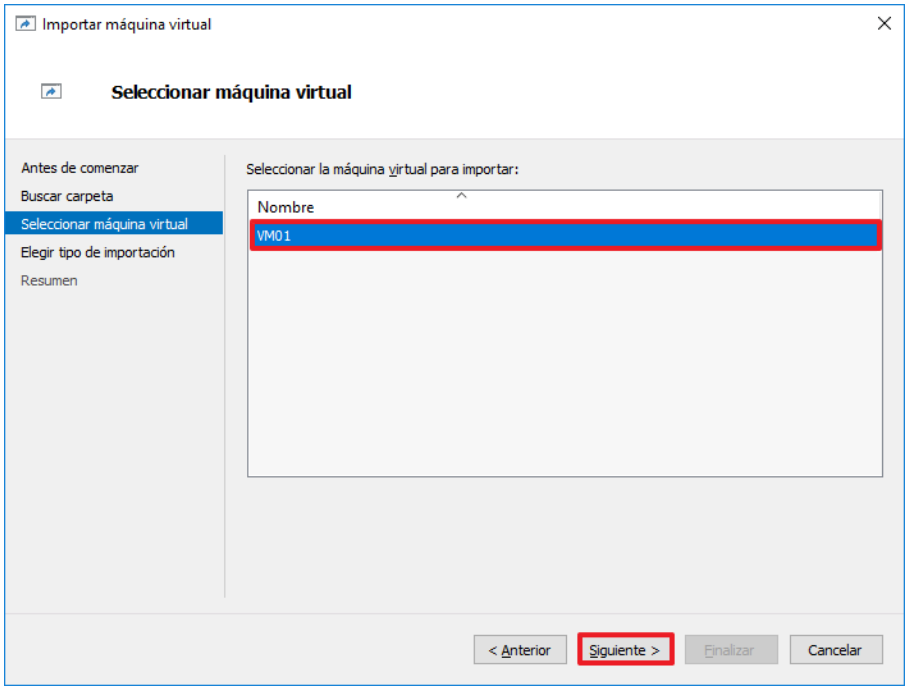
Paso	Descripción
115.	Pulse sobre el botón “Exportar” para comenzar con la copia. 
116.	Cuando el proceso haya finalizado la consola de Hyper-V lo notificará en el apartado correspondiente al “Estado” y dentro del directorio seleccionado se habrá generado un directorio con todos los componentes de la máquina virtual.  **Nota:** Dependiendo del tamaño de la máquina el tiempo podrá variar. La consola de Hyper-V mostrará en todo caso el porcentaje de estado. 

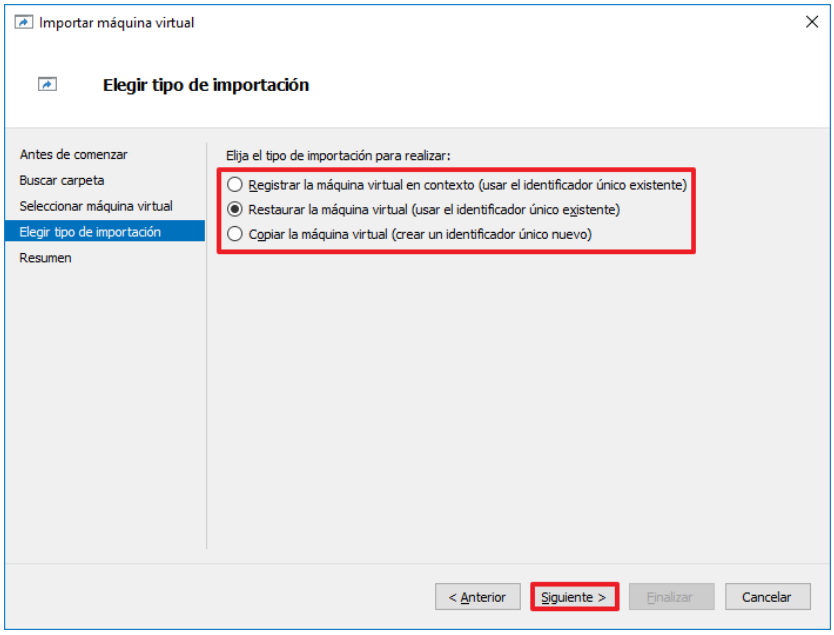
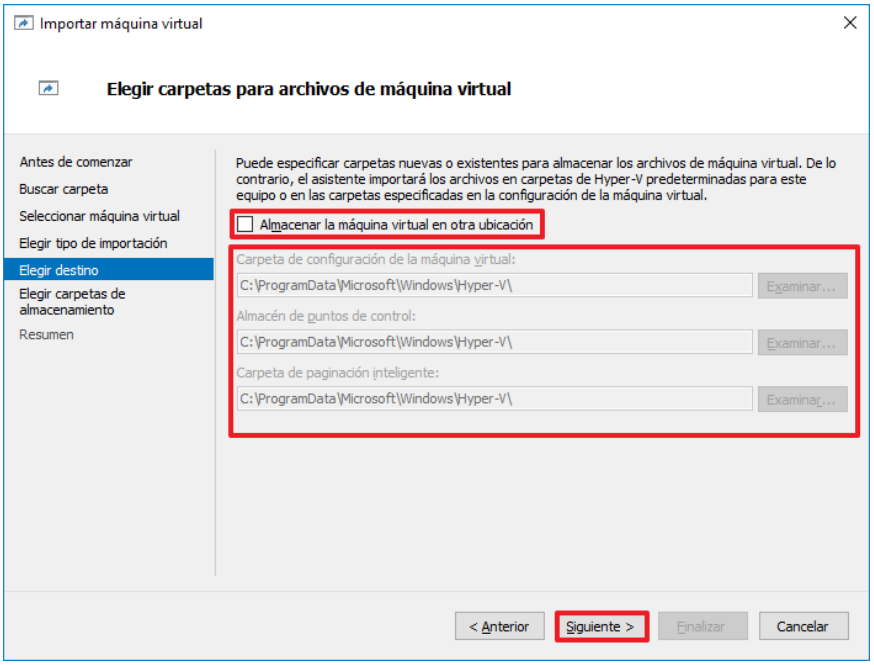
2.7.2. IMPORTAR MÁQUINAS VIRTUALES

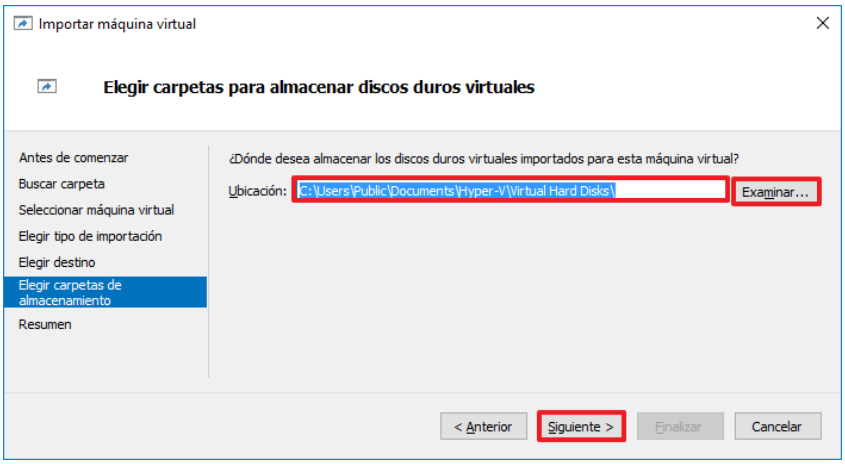
Paso	Descripción
117.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
118.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
119.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 

Paso	Descripción
120.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
121.	Seleccione la opción del panel derecho "Importar máquina virtual…". 
122.	Se iniciará el asistente para importar una máquina virtual. Pulse "Siguiente >" en la ventana "Antes de comenzar".

Paso	Descripción
123.	En la ventana “Buscar carpeta” pulse sobre el botón “Examinar…”. 
124.	A continuación, seleccione el directorio donde se encuentre la máquina virtual y pulse sobre “Seleccionar carpeta”.  **Nota:** Si selecciona una ubicación incorrecta el asistente notificará un error. 

Paso	Descripción
125.	Pulse el botón “Siguiente >” para continuar con la importación. 
126.	Seleccione la máquina virtual que desea importar y pulse “Siguiente >”.  **Nota:** Es posible que la ruta indicada posea varias máquinas virtuales para importar, por lo que deberá seleccionar aquella que corresponda.

Paso	Descripción
127.	En la ventana elegir tipo de importación seleccione la opción más adecuado dependiendo de la operación a realizar con la máquina. Pulse “Siguiente >” para finalizar con la importación”.  **Nota:** En este ejemplo se hace uso de la opción “Restaurar la máquina virtual”. Dependiendo de la opción seleccionada deberá ejecutar más o menos pasos en el asistente.
128.	En la ventana “Elegir destino” deberá establecer si lo desea una ruta para cada una de las configuraciones de la máquina virtual. Pulse “Siguiente >” cuando haya finalizado.  **Nota:** En este ejemplo se opta por ubicar los archivos en las rutas por defecto definidas en apartados anteriores.

Paso	Descripción
129.	Al igual que sucedía en el paso anterior deberá ahora establecer la ubicación para los discos de la máquina virtual. Si no indica dicha ubicación se almacenarán en la ubicación predefinida en apartados anteriores. Pulse “Siguiente >” para continuar. 
130.	Por último, en la ventana “Resumen” compruebe que las configuraciones de la máquina virtual son correctas. En caso afirmativo pulse “Finalizar”. Si por el contrario requiere modificar alguna configuración pulse el botón “< Anterior” hasta llegar a la ventana deseada y modifique la configuración.

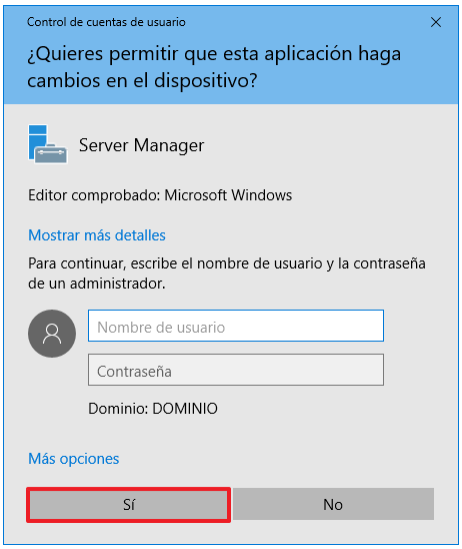
2.8. DERECHOS DE ACCESO SOBRE SISTEMAS OPERATIVOS MS WINDOWS VIRTUALIZADOS

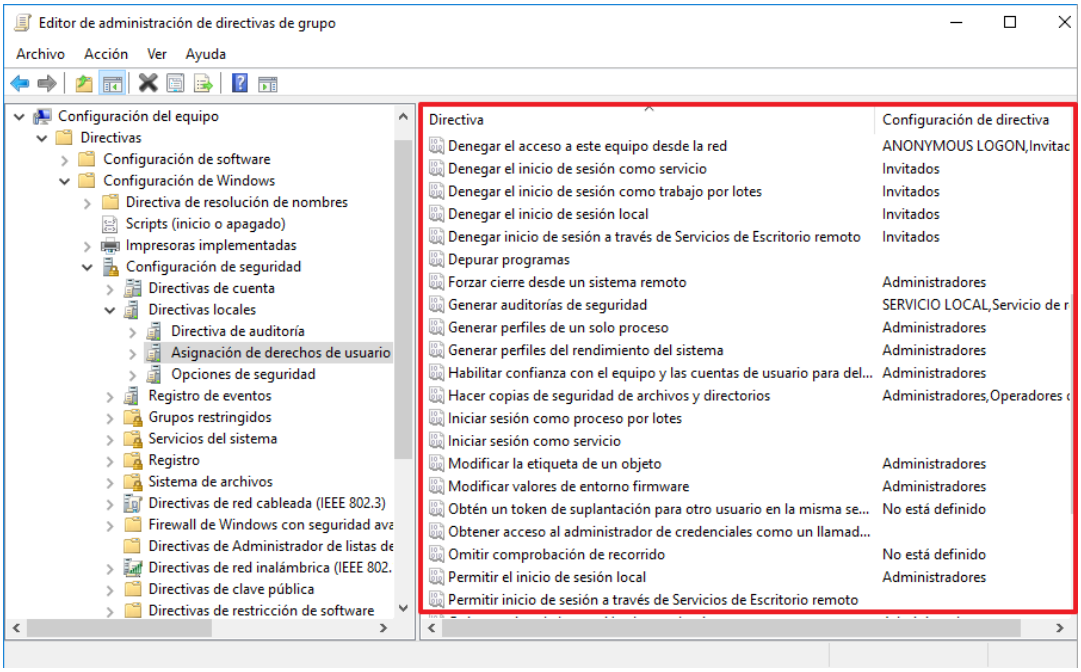
Los permisos de acceso sobre las máquinas virtuales que contiene el servicio de Hyper-V debe quedar limitado a los usuarios legítimos a ello por lo tanto será necesario establecer los permisos necesarios para limitar dicha conectividad.

Deberá tener en consideración la asignación de permisos diferenciando si la conexión se realiza a un servidor o un equipo cliente. Deberá por tanto generar un objeto GPO incremental o modificar la configuración establecida con el fin de permitir o denegar el inicio de sesión sobre las máquinas virtuales.

En el presente apartado se trata el ejemplo de configurar dicha asignación de permisos a través del objeto GPO que configura Hyper-V.

Paso	Descripción
131.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS. **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
132.	Ejecute el “Administrador del Servidor” desde el icono correspondiente. 

Paso	Descripción
133.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
134.	A continuación, inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor”, abierta en pasos anteriores, seleccione **“Herramientas → Administración de directivas de grupo”.** 
135.	Los objetos de políticas de grupo para Controladores de Dominio y Servidores miembros especifican unos derechos de usuario siguiendo planteamientos de seguridad que aplican los principios de mínimo privilegio y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les hayan asignado derechos determinados para la administración o gestión de los sistemas. Si esto fuera así, deberá realizar las modificaciones pertinentes sobre el objeto de política de grupo que aplique sobre el sistema operativo virtualizado o bien editando la configuración de política de grupo local en el caso de un equipo no perteneciente a un dominio.
136.	Sobre el objeto de GPO que se quiere modificar, deberá pulsar clic derecho y seleccionar “Editar” en el menú desplegado.

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

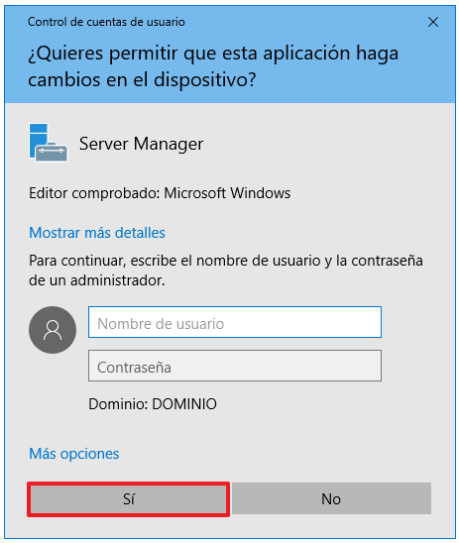
2.9. ACCESO REMOTO SOBRE SISTEMAS OPERATIVOS MS WINDOWS VIRTUALIZADOS

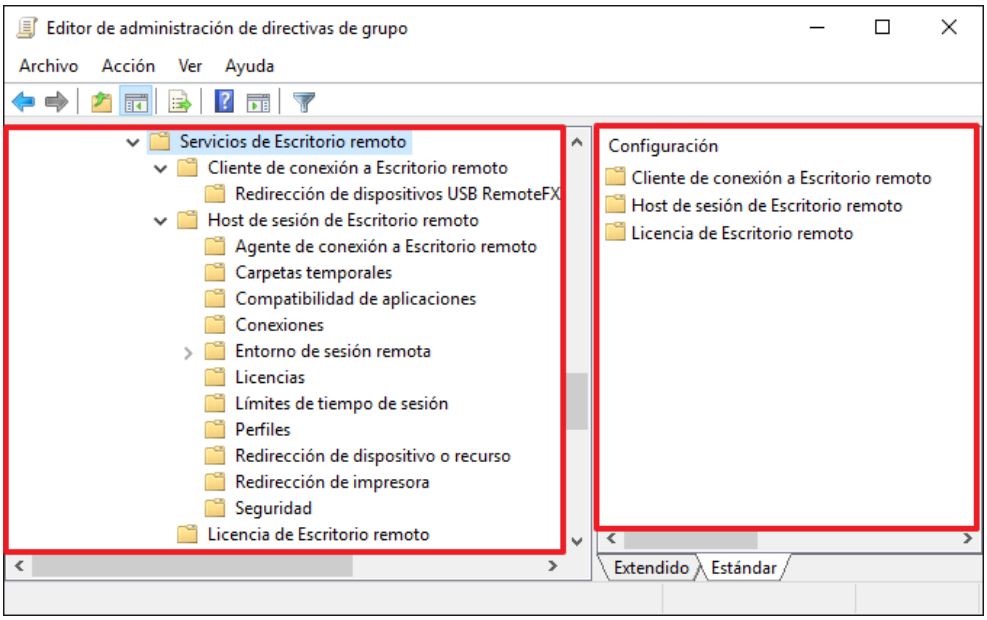
Del mismo modo que en el punto anterior no basta con conceder permisos sobre los equipos cliente o servidores ubicados dentro del servidor de Hyper-V sino que además será necesario establecer los mecanismos seguros para las conexiones remotas a las máquinas virtuales que almacena Hyper-V.

En el presente apartado se definen las medidas a tomar en el caso de realizar una conexión remota a través del servicio Escritorio Remoto de Windows. Para definir dicha configuración deberá hacer uso de un objeto GPO incremental que configure la seguridad de dicho servicio o editar la configuración de un objeto GPO ya aplicado.

Para el presente ejemplo se realiza un ejemplo de configuración para escritorio remoto que asegure la conexión de este servicio al servidor de Hyper-V.

Paso	Descripción
140.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS. **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

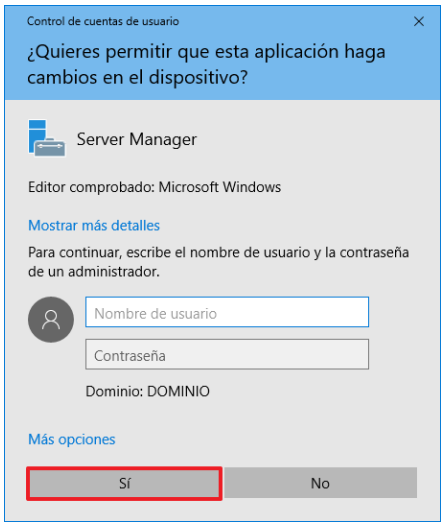
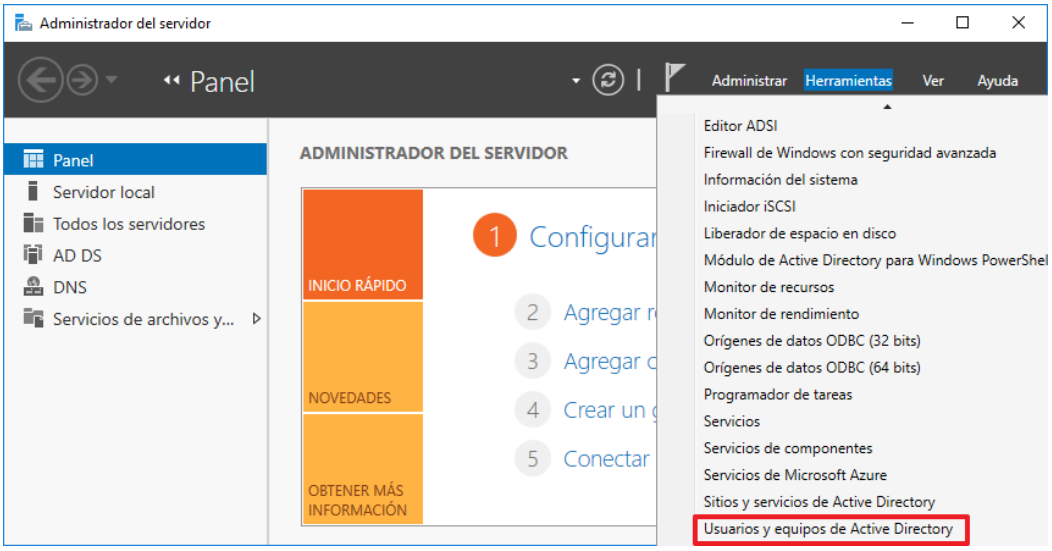
Paso	Descripción
141.	Ejecute el “Administrador del Servidor” desde el icono correspondiente. 
142.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí”. 
143.	A continuación, inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor”, abierta en pasos anteriores, seleccione **“Herramientas → Administración de directivas de grupo”.** 
144.	Los elementos de plantillas administrativas permiten establecer la configuración segura a realizar sobre una conexión basada en servicios de escritorio remoto. Esta configuración permite que las conexiones realizadas a servidores y equipos cliente asegure la integridad de la conexión. Para establecer dicha configuración, deberá realizar las modificaciones pertinentes sobre el objeto de política de grupo que aplique sobre el sistema operativo virtualizado o bien editando la configuración de política de grupo local en el caso de un equipo no perteneciente a un dominio.
145.	Sobre el objeto de GPO que se quiere modificar, deberá pulsar clic derecho y seleccionar “Editar” en el menú desplegado.

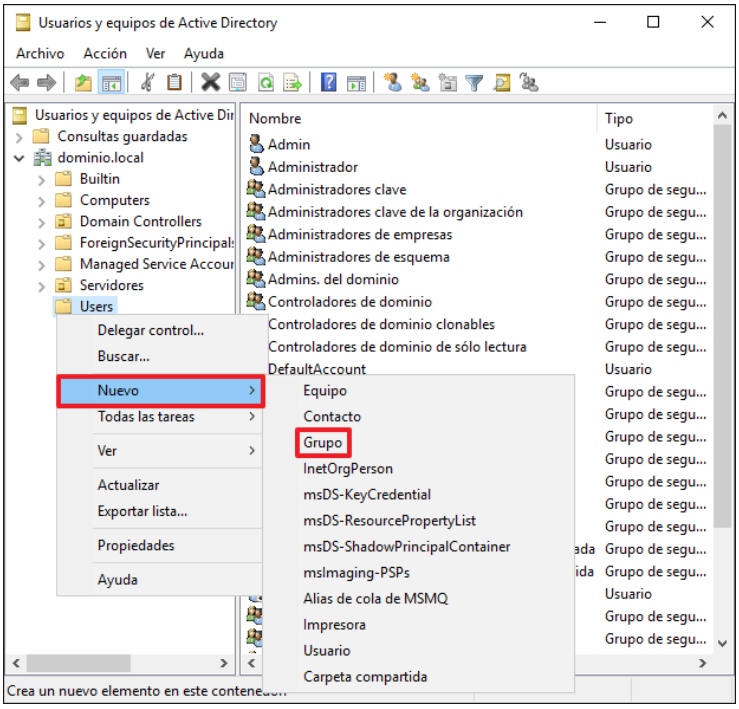
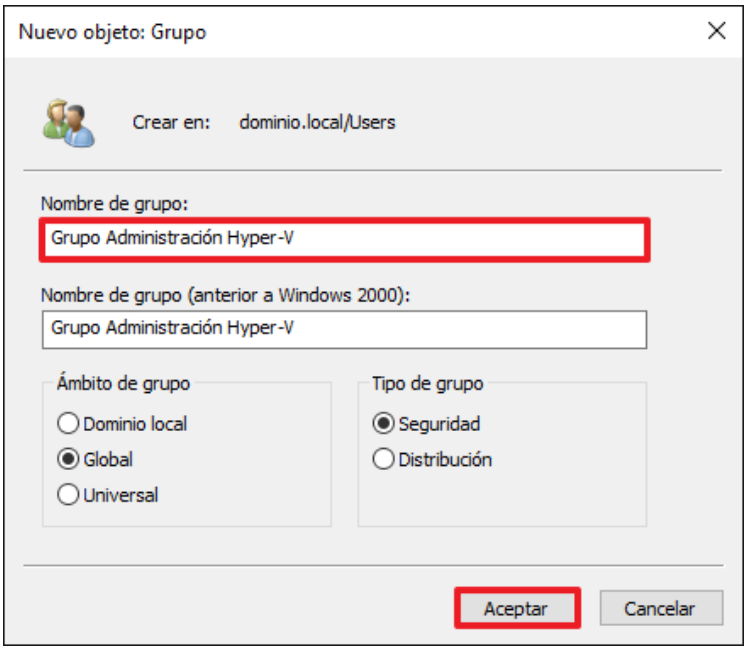
Paso	Descripción
146.	Una vez abierto el "Editor de administración de directivas de grupo", despliegue la política y sitúese en la siguiente ruta. **"Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Servicios de Escritorio remoto"** 
147.	Modifique las directivas, estableciendo una configuración segura para el acceso remoto tanto a servidores como equipos cliente.
148.	Guarde la configuración cerrando la ventana de editor de administración de directivas de grupo.
149.	Adicionalmente a esta configuración deberá establecer los parámetros de red que permitan realizar la comunicación en red. Para ello haga uso de nuevo del objeto GPO correspondiente y configurando el firewall para que permita la conexión entre equipos.
150.	Como última medida, y que es aplicable a partir la categoría media del ENS, deberá establecer las acciones permitidas y acciones no permitidas por la política de la organización durante el acceso remoto a las máquinas virtuales.

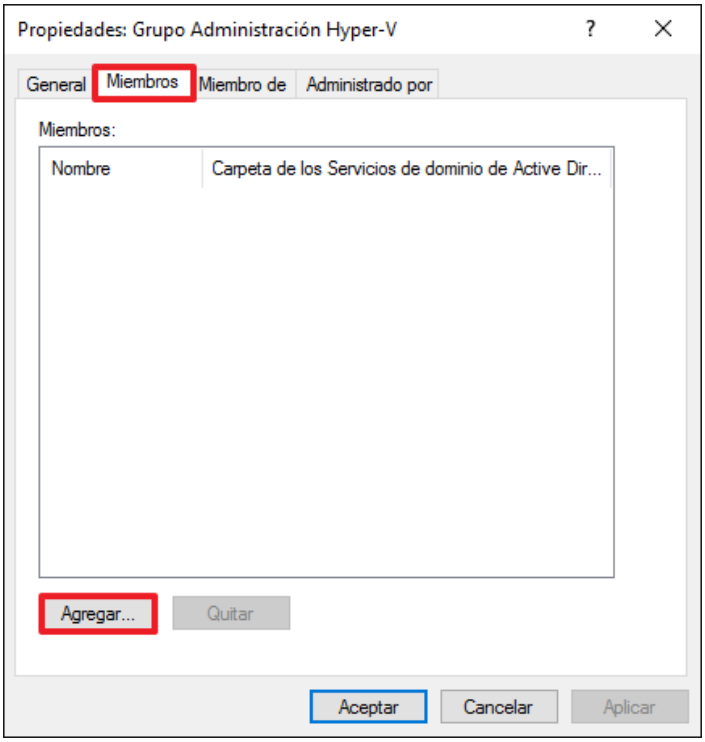
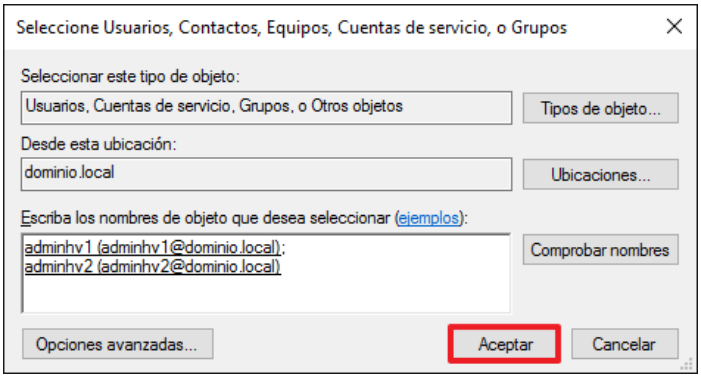
2.10. SEGREGACION DE ROLES

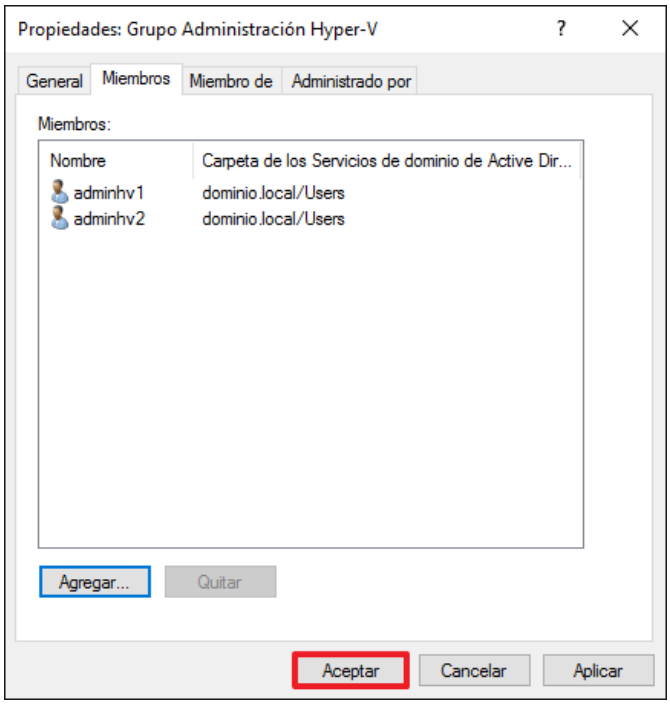
A partir de la aplicación del ENS para la categoría media sobre el Servidor de Hyper-V será necesario crear grupos de usuarios para conceder permisos de administración sobre Hyper-V.

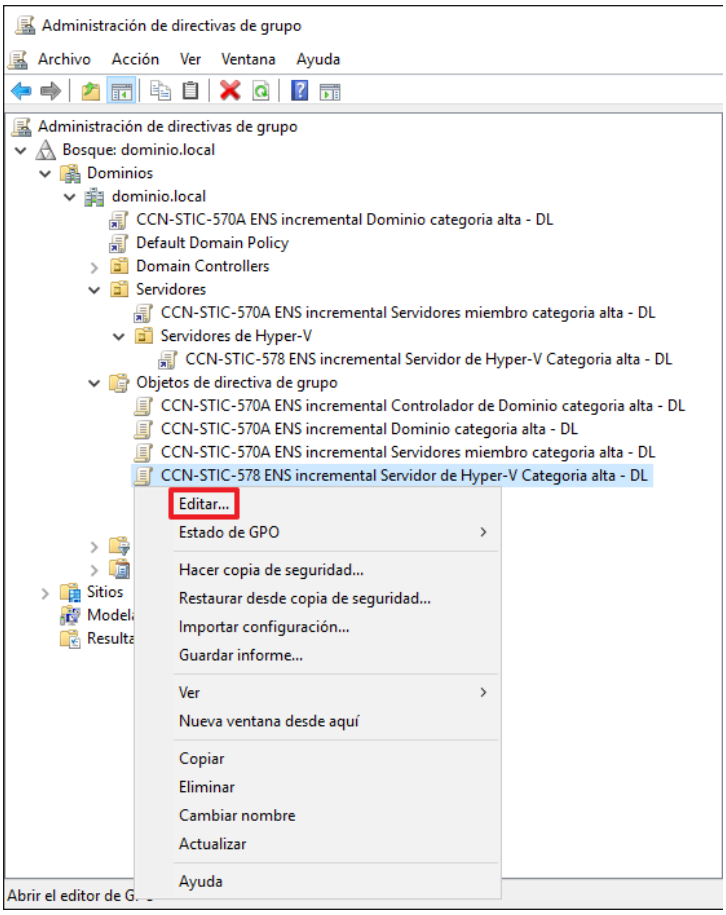
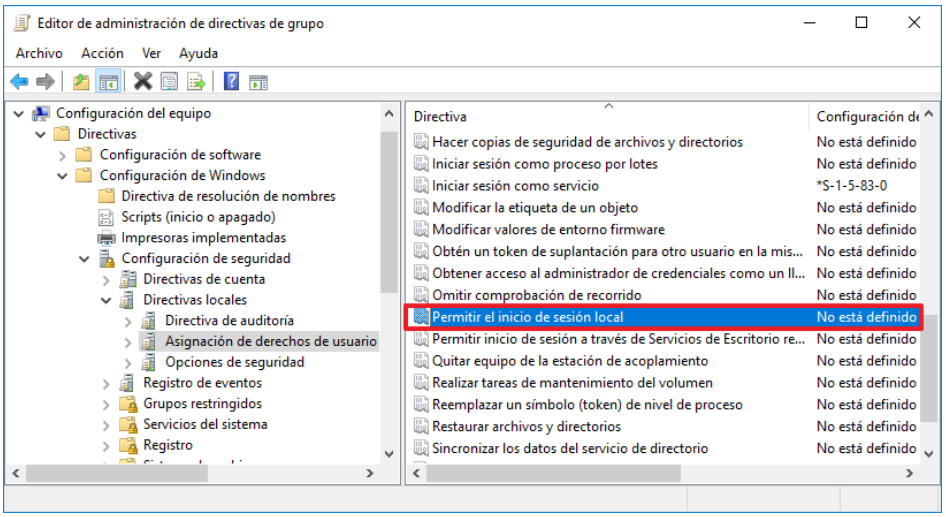
Paso	Descripción
151.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS. **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
152.	Ejecute el "Administrador del Servidor" desde el icono correspondiente. 

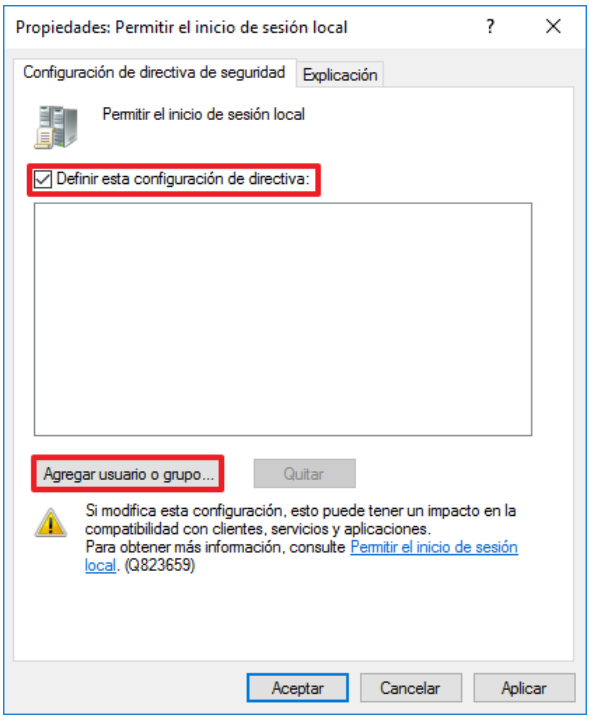
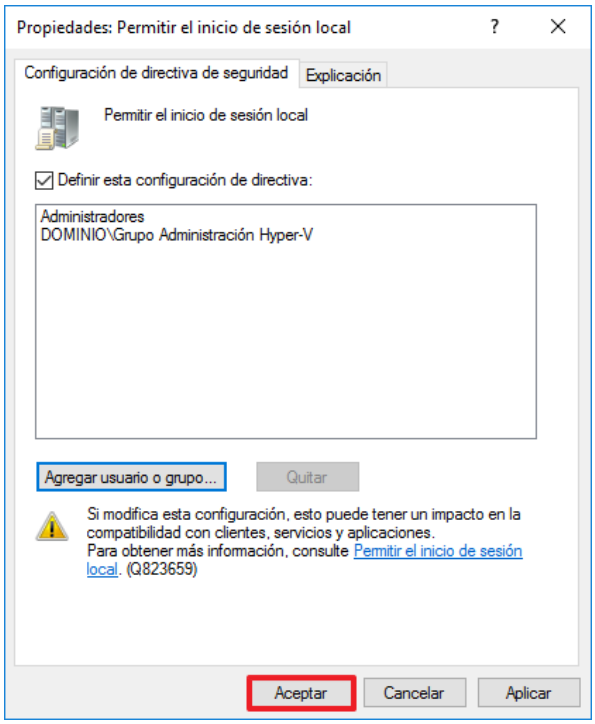
Paso	Descripción
153.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
154.	Inicie la herramienta “Usuarios y equipos Active Directory”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Usuarios y equipos de Active Directory”**. 

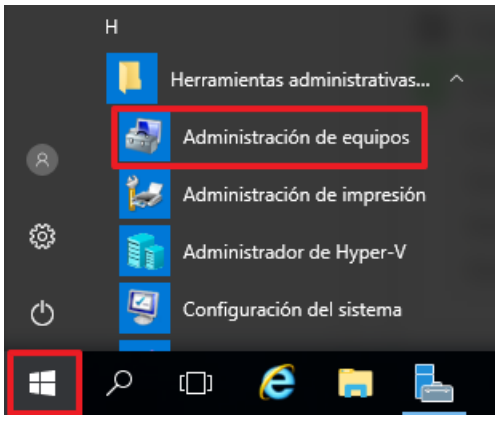
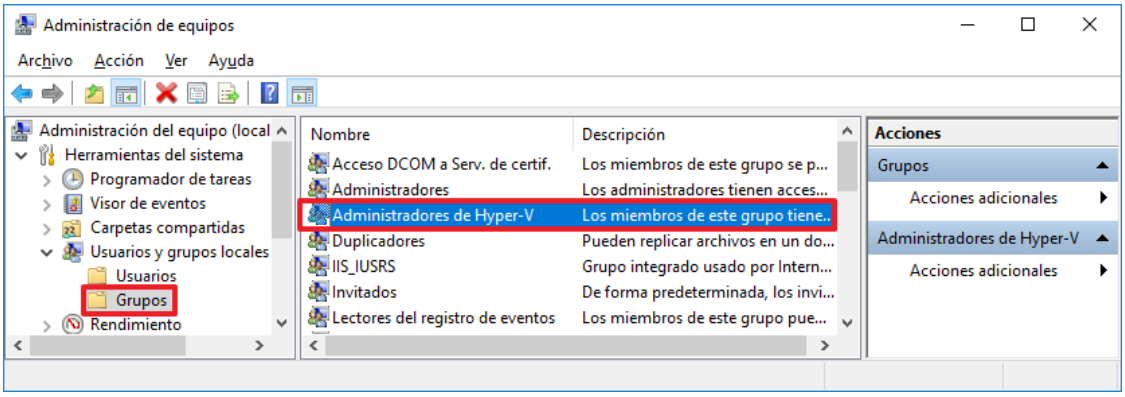
Paso	Descripción
155.	Despliegue el nodo **"<<su dominio>> → Users"**. Pulse con el botón derecho sobre "Users" y seleccione la opción del menú contextual **"Nuevo → Grupo"**. 
156.	Establezca el nombre de grupo deseado para su organización y pulse "Aceptar".  **Nota:** En este ejemplo se utiliza el nombre "Grupo Administración Hyper-V".

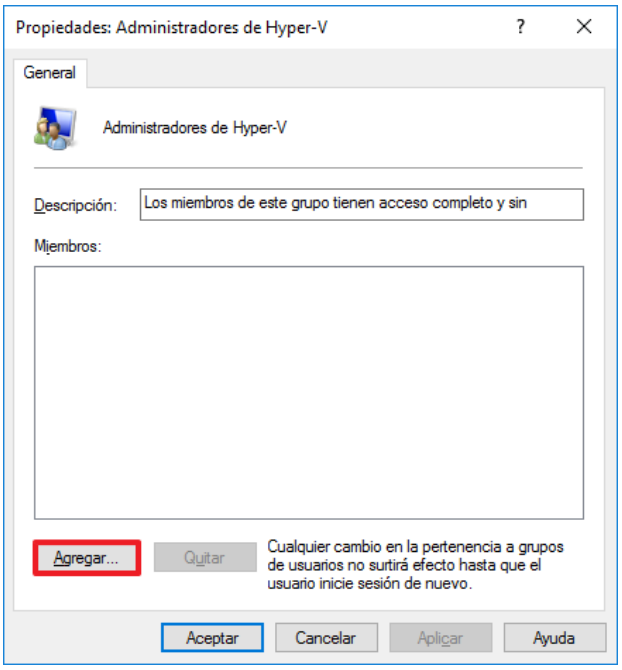
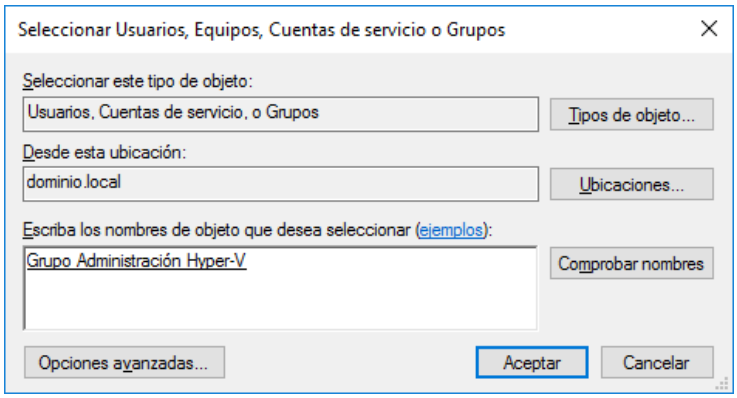
Paso	Descripción
157.	Haga doble clic sobre el grupo recién creado y acceda a la pestaña “Miembros”. Pulse sobre el botón “Agregar…” para añadir usuarios al grupo. 
158.	Añada los usuarios que desee al grupo y pulse “Aceptar”.  **Nota:** En este ejemplo se añaden los usuarios “adminhv1” y “adminhv2” utilizados para la creación de esta guía.”

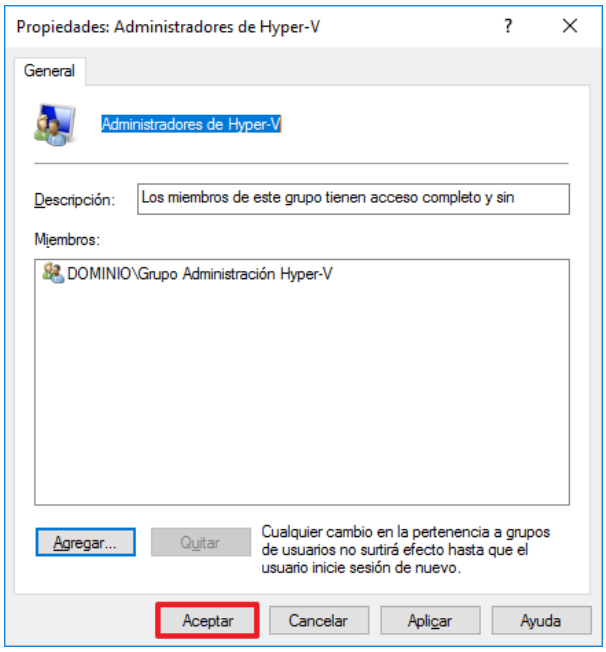
Paso	Descripción
159.	Pulse “Aceptar” cuando haya finalizado. 
160.	A continuación, inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor”, abierta en pasos anteriores, seleccione **“Herramientas → Administración de directivas de grupo”.** 

Paso	Descripción
161.	Acceda al nodo “Objetos de directiva de grupo”, pulse con el botón derecho el objeto GPO denominado “CCN-STIC-578 incremental Servidor de Hyper-V Categoria alta - DL”, creado en apartados anteriores y seleccione la opción del menú contextual “Editar…”. 
162.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”**. Haga doble clic en el panel derecho sobre la directiva **“Permitir el inicio de sesión local”**. 

Paso	Descripción
163.	Marque la casilla “Definir esta configuración de directiva:” y pulse sobre “Agregar usuario o grupo…”. 
164.	Agregue el grupo “Administradores” y aquellos usuarios o grupos delegados para la administración del servidor de Hyper-V. Pulse “Aceptar” cuando haya finalizado.  **Nota:** En este ejemplo se hace uso del grupo denominado “Grupo Administración Hyper-V”. Deberá adaptar esta configuración a las necesidades de su organización.

Paso	Descripción
165.	A continuación, inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
166.	Pulse sobre "Inicio" y seleccione **"Herramientas administrativas → Administración de equipos"**. 
167.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con privilegios de administrador y pulse "Sí" para continuar.
168.	Despliegue el nodo **"Administración del equipo (local) → Herramientas del sistema → Usuarios y grupos locales → Grupos" y haga doble clic sobre el grupo "Administradores de Hyper-V"**. 

Paso	Descripción
169.	En la ventana emergente pulse sobre “Agregar…”. 
170.	Agregue los usuarios o grupo pertenecientes al dominio que tengan como privilegio la administración del servidor de Hyper-V.  **Nota:** En este ejemplo se hace el grupo denominado “Grupo Administración Hyper-V” creado para tal propósito. Los usuarios o grupos aquí introducidos deberán coincidir con lo introducidos en el paso 164 para permitir la administración de lo contrario ésta no será posible.

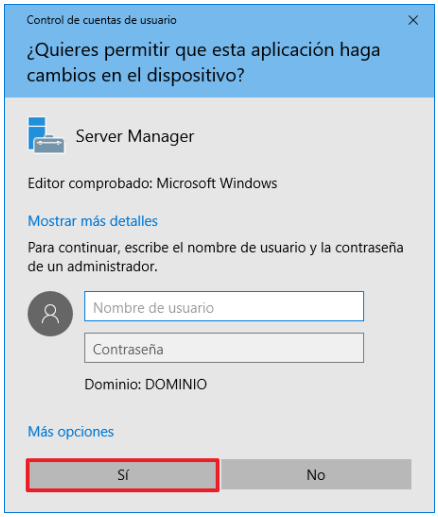
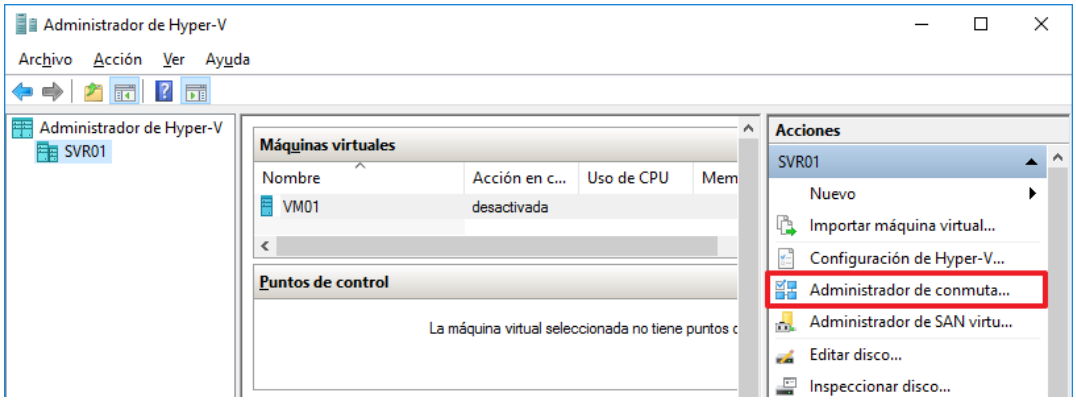
Paso	Descripción
171.	Cuando haya finalizado pulse “Aceptar” para guardar la configuración. 
172.	A partir de este momento los usuarios pertenecientes al grupo definido como “Grupo Administración Hyper-V” podrán acceder al servidor de Hyper-V y administrar dicho rol.

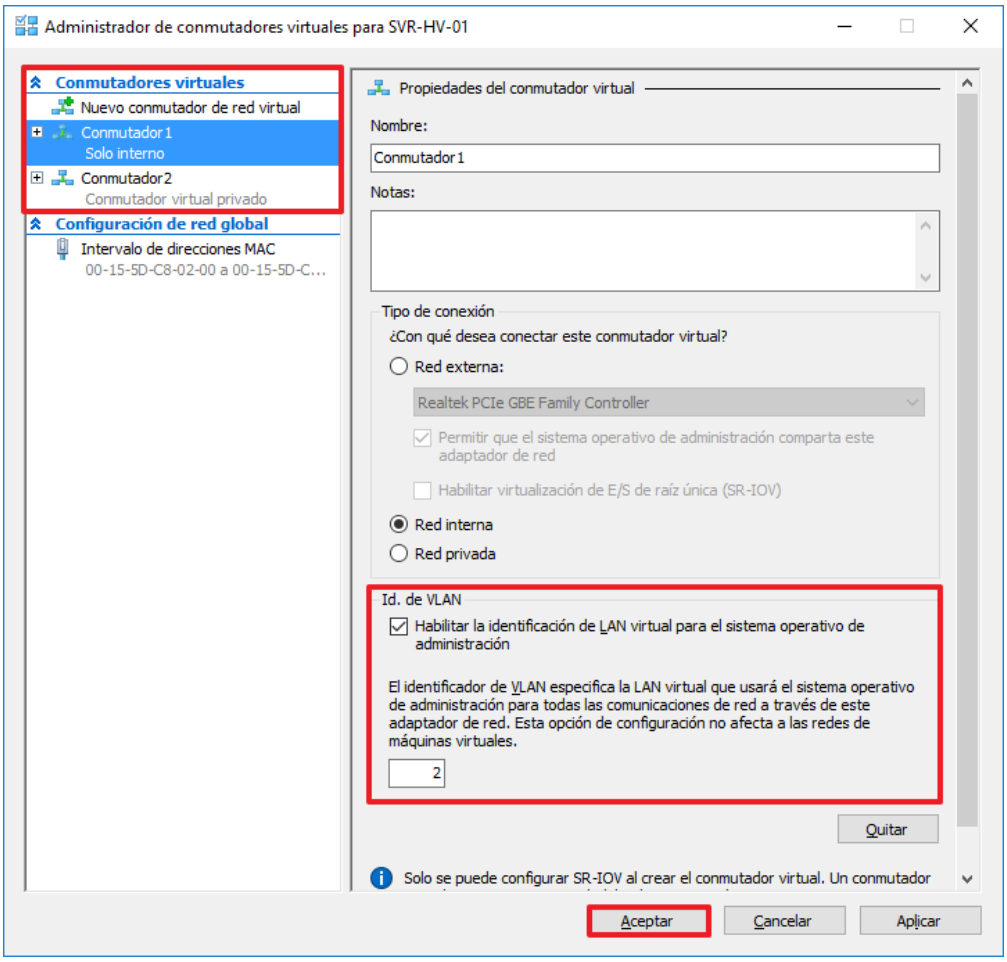
2.11. SEGREGACIÓN DE REDES

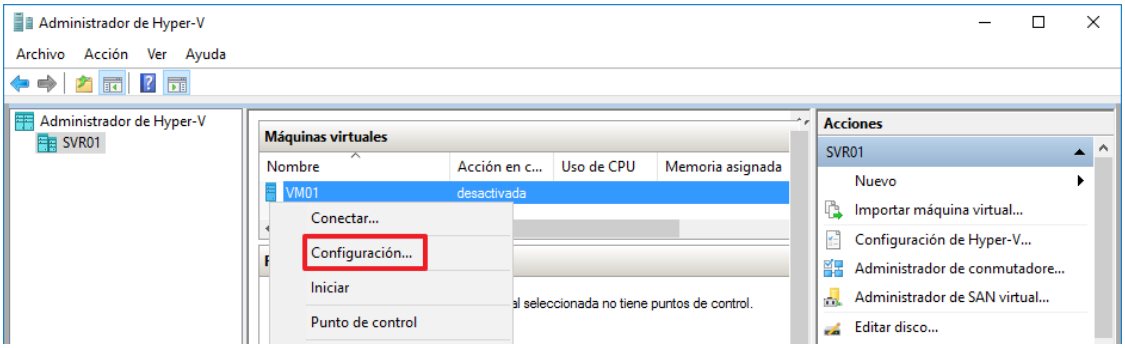
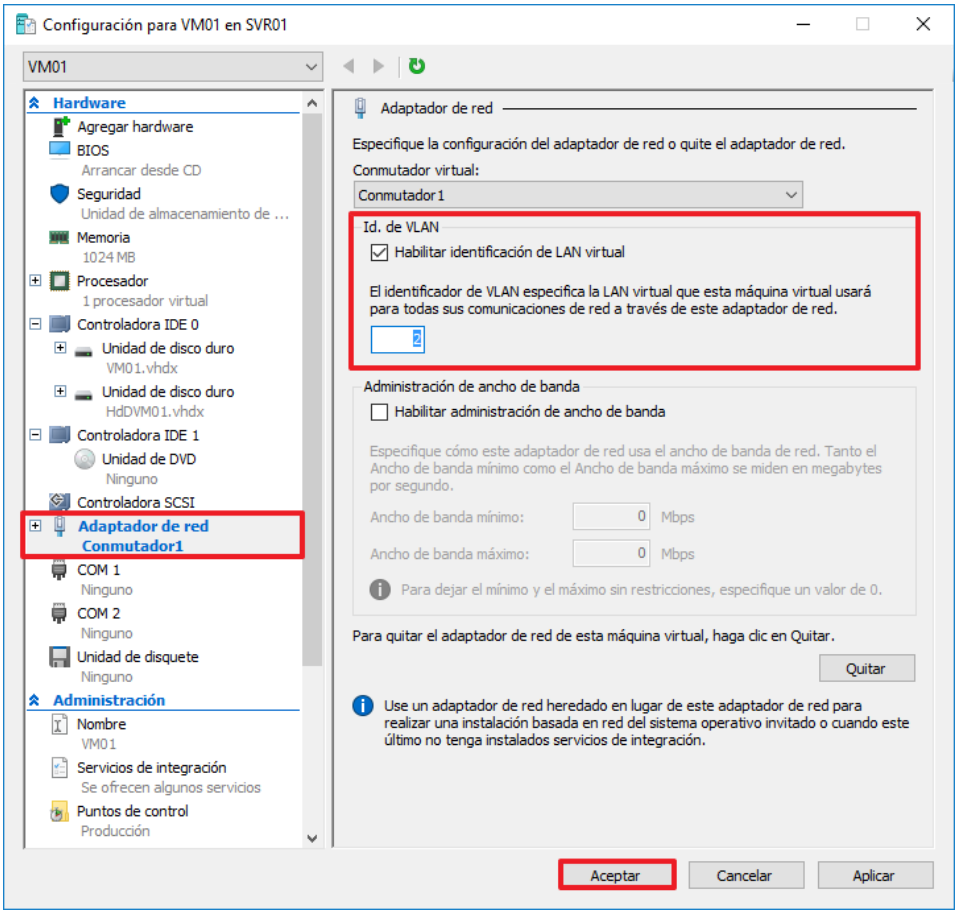
Dentro de la categoría alta del ENS se define la necesidad de realizar una segregación de las redes definidas en las diferentes máquinas virtuales con el objeto de dividir el tráfico de red y garantizar la integridad y confidencialidad de los datos intercambiados.

Nota: Deberá determinar en quien es delegada la tarea de gestión de VLAN’s ya que es posible que esta configuración no se adapte a las necesidades de su organización debido a que se posean otros dispositivos como un Switch que realice dicha gestión. En cualquier caso, deberá garantizar en todo momento la segregación de las redes disponibles dentro de su organización.

Paso	Descripción
173.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

Paso	Descripción
174.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
175.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
176.	Inicie la herramienta “Administrador de Hyper-V”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administrador de Hyper-V”**. 
177.	Dentro de la consola emergente seleccione el servidor de Hyper-V instalado en el servidor y a continuación en el panel de “Acciones” seleccione la opción “Administrador de conmutadores virtuales”. 

Paso	Descripción
178.	Deberá establecer la configuración de VLAN en sus adaptadores de tipo “Interno” y “Externo” activando la opción “Habilitar la identificación de LAN virtual para el sistema operativo de administración” y definiendo el número de VLAN correspondiente a la segregación a realizar.  **Nota:** Esta configuración será necesario en caso de que el host deba establecer comunicación con las máquinas virtuales que contiene, con el fin de compartir el tráfico si van a encontrarse dentro de la misma red. Deberá tener en consideración adicionalmente, en el caso de un conmutador “Externo” la opción de permitir o denegar la compartición del adaptador de red. En este ejemplo se toma como identificador VLAN específica la LAN Virtual 2, que dicha máquina virtual usará para todas sus comunicaciones en la red a través de su adaptador de red. Deberá adaptar la configuración de VLAN según las necesidades de su organización.
179.	Adicionalmente en los adaptadores asociados a cada máquina virtual deberá establecer del mismo modo que sobre el conmutador virtual, la VLAN asociada a dicho adaptador de red y que permitirá realizar la segregación de la red.

Paso	Descripción
180.	Para ello haga clic derecho sobre la máquina deseada y seleccione la opción del menú contextual "Configuración…". 
181.	Dentro del apartado "Adaptador de red" seleccione el conmutador asociado a la máquina y marque la opción "Habilitar identificación de LAN virtual". Por último, defina el número de VLAN asociada. 
182.	Así mismo deberá configurar las máquinas virtuales de forma que posean el conmutador de red adecuado.

ANEXO A.4.2. LISTA DE COMPROBACIÓN DE HYPER-V SOBRE WINDOWS SERVER 2016 PARA SERVIDORES QUE LES SON DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía "ANEXO A.4.1 PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE HYPER-V SOBRE SERVIDORES WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA".

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

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

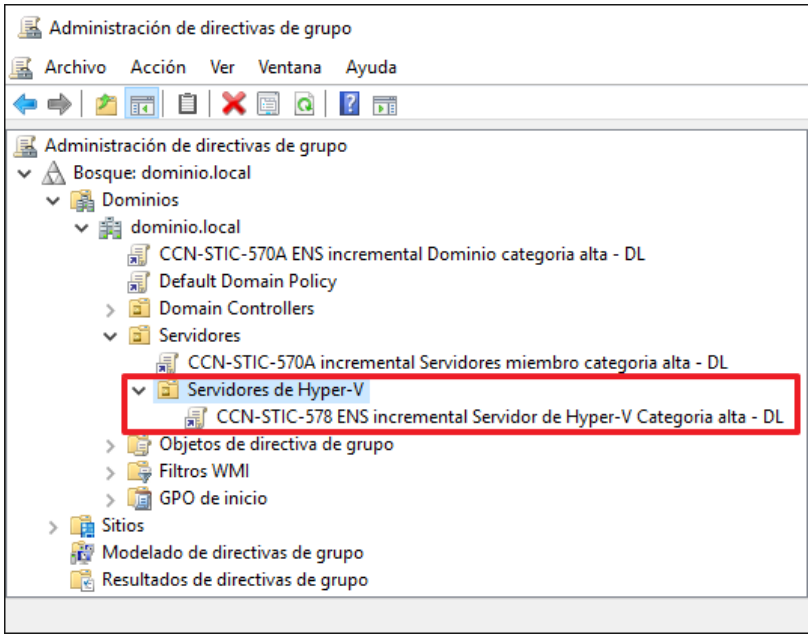
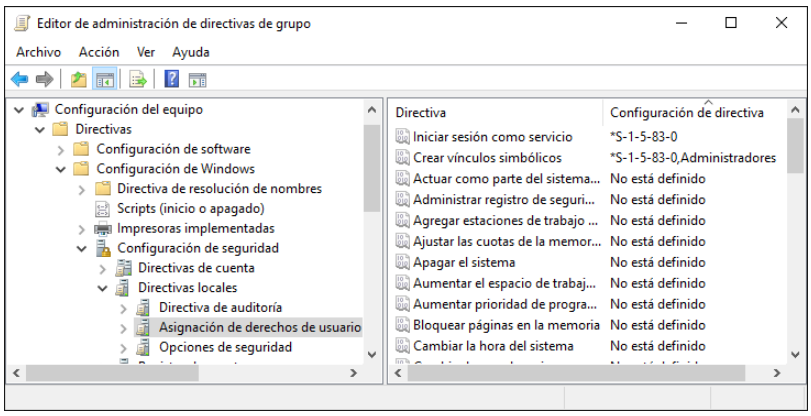
Posteriormente, se deberán realizar las comprobaciones en el propio servidor de Hyper-V, para lo que será necesario ejecutar diferentes consolas de administración y herramientas del sistema, las cuales estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario con privilegios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

a) En el Controlador de Dominio:
   i. Usuarios y equipos de Active Directory (dsa.msc).
   ii. Administrador de directivas de grupo (gpmc.msc).
   iii. Editor de objetos de directiva de grupo (gpedit.msc).

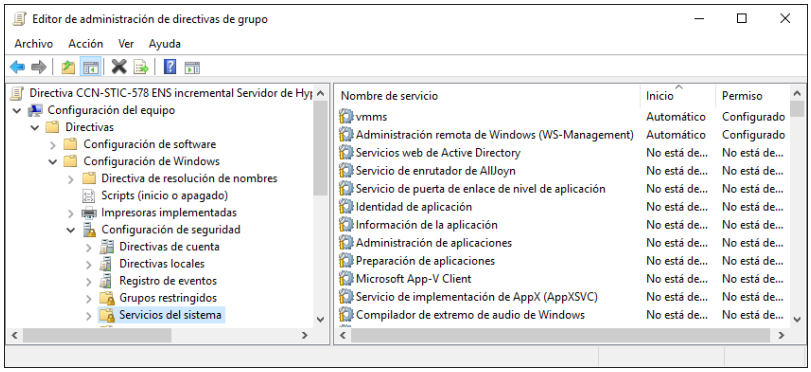
b) En el servidor de Hyper-V:
   i. Administrador de Windows (explorer.exe).
   ii. PowerShell (powershell.exe).
   iii. Servicios (services.msc).
   iv. Editor de objetos de directiva de grupo (gpedit.msc).
   v. Administrador de Hyper-V (virtmgmt.msc).
   vi. Visor de eventos (eventvwr.msc).

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

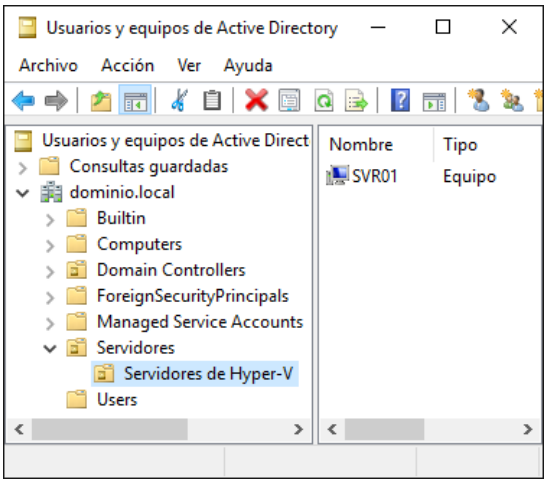
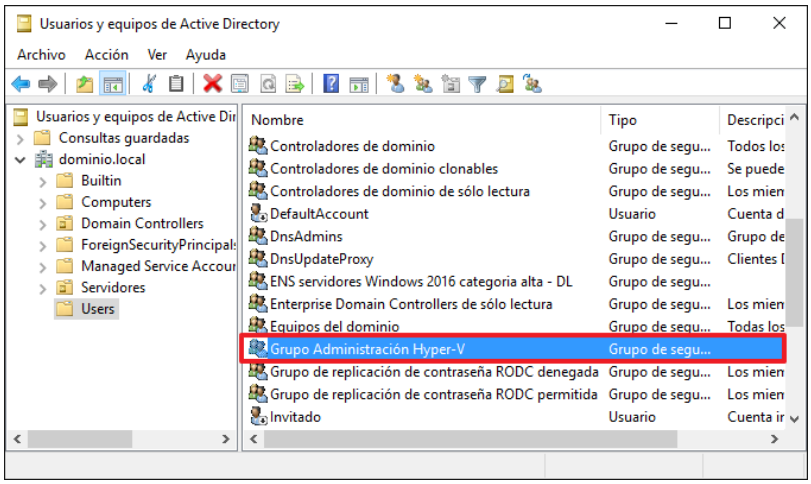
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un Controlador de Dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.

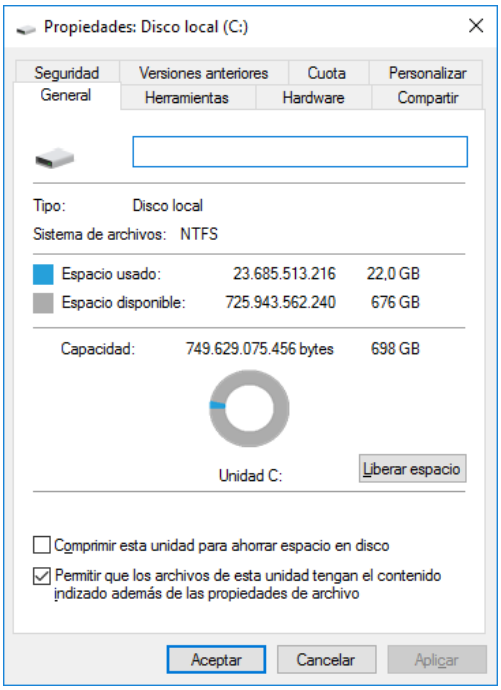
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>2. Verifique que está creada la directiva “CCN-STIC-578 ENS incremental Servidor de Hyper-V Categoria alta - DL”.</td><td></td><td>Utilice el Administrador de directivas de grupo (Inicio → Herramientas administrativas → Administración de directivas de grupo) y despliegue el menú en árbol hasta llegar a la unidad organizativa “Servidores de Hyper-V” que se encuentra en la Unidad Organizativa “Servidores”. Verifique que está creada la política “CCN-STIC-578 ENS incremental Servidor de Hyper-V Categoria alta - DL”.
 
</td></tr>
<tr><td>3. Verifique los valores de la asignación de derechos de usuario.</td><td></td><td>Utilizando el editor de objetos de directiva de grupo, verifique que la directiva “CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria alta - DL” tiene los siguientes valores de asignación de derechos de usuario en el siguiente nodo:
Directiva CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria alta - DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Iniciar sesión como servicio</td><td>Máquinas virtuales (*S-1-5-83-0)</td><td></td></tr>
<tr><td>Crear vínculos simbólicos</td><td>Máquinas virtuales (*S-1-5-83-0)
Administradores</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
4. Verifique los valores de servicios.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria alta - DL" tiene los siguientes valores de asignación de derechos de usuario en el siguiente nodo: **Directiva CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria alta - DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del Sistema.** 

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Administración de máquinas virtuales de Hyper-V	vmms	Automático	Configurado	
Agente de host NC	nchostagent	Deshabilitado	Configurado	
Aislamiento de claves CNG	keyiso	Automático	Configurado	
Instantáneas de volumen	vss	Manual	Configurado	
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado	
Servicio de cierre de invitado de Hyper-V	vmicshutdown	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado	
Servicio de proceso de host de Hyper-V	vmcompute	Manual	Configurado	
Servicio de proxy DNS	DNSProxy	Deshabilitado	Configurado	
Servicio de red de host	hns	Manual	Configurado	
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado	
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual	Configurado	
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado	
Software Load Balancer Host Agent	SlbHostAgent	Manual	Configurado	

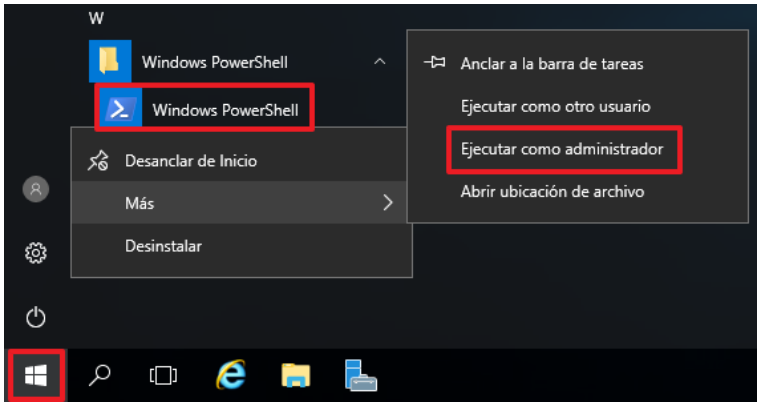
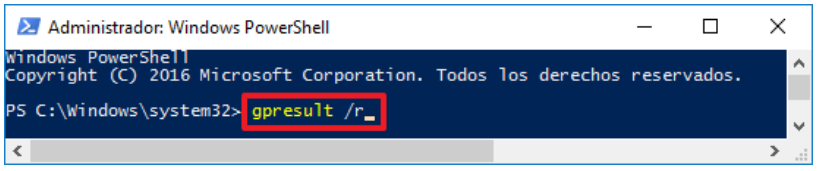
Comprobación	OK/NOK	Cómo hacerlo
5. Verifique que los servidores de Hyper-V están dentro de las Unidades Organizativas adecuada		Utilice la herramienta Usuarios y equipos de Active Directory (**Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**) y seleccione las unidades organizativas que contienen los Servidores de Hyper-V. Compruebe que existe un objeto de tipo equipo por cada uno de los servidores de Hyper-V que se están asegurando.  **Nota:** Para el desarrollo de esta guía se utiliza la Unidad Organizativa "Servidores de Hyper-V".
6. Verifique que existe un grupo dedicado para la administración de Hyper-V		Utilice la herramienta Usuarios y equipos de Active Directory (**Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**) y verifique que existe al menos un grupo dedicado a la administración del Servidor de Hyper-V.  **Nota:** El nombre del grupo y los usuarios pertenecientes al grupo variará dependiendo de la configuración aplicada en su organización
7. Inicie sesión en un Servidor de Hyper-V		Para completar el resto de la lista de verificación deberá iniciar sesión con una cuenta que tenga permisos de administrador del dominio.

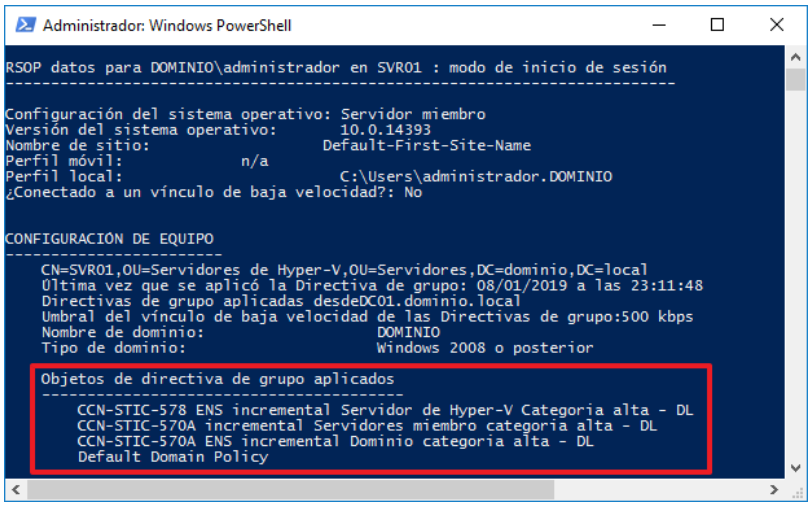
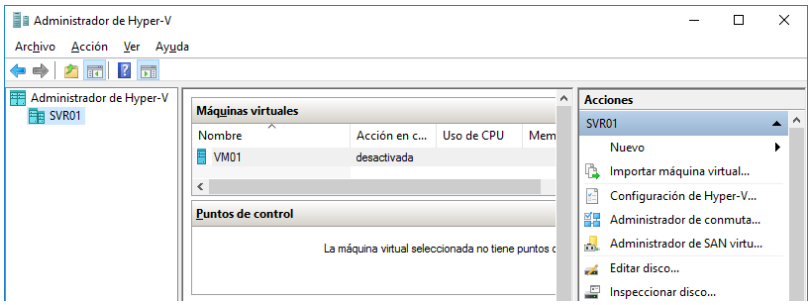
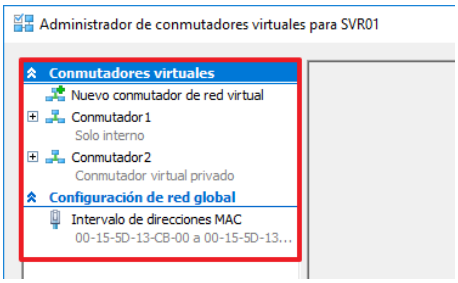
Comprobación	OK/NOK	Cómo hacerlo
8. Verifique el sistema de ficheros de los volúmenes		Utilizando el explorador de Windows (botón derecho sobre **Inicio → Explorador de archivos**, botón derecho sobre la unidad C:\), verifique en las propiedades de cada partición el uso del sistema de archivos NTFS o cualquier sistema de archivos que permita la aplicación de ACL's. 
9. Verifique que están instalados los componentes que se indican		En el "Administrador del Servidor", pulse sobre la opción "Servidor Local" situado en el lateral izquierdo y diríjase a la parte final de la ventana principal, "Roles y características", por medio del scroll lateral derecho. Compruebe que se encuentran instalados los siguientes componentes.

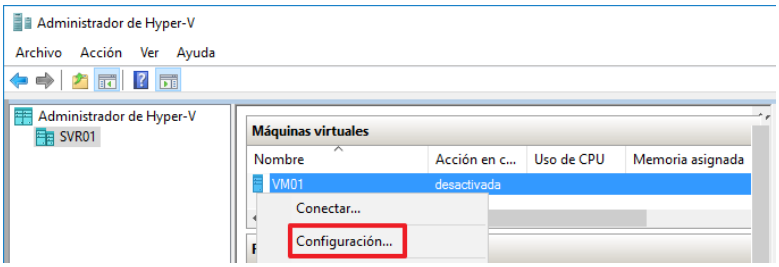
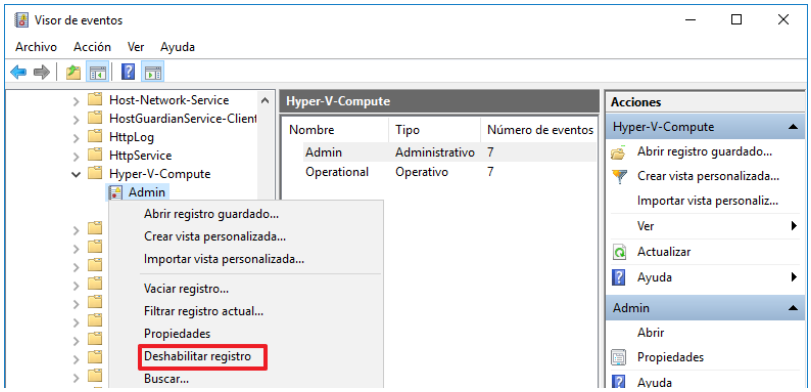
Rol	OK/NOK
Hyper-V	

10. Verifique los valores de servicios.		Ejecute el complemento "Servicios" (ejecutando "services.msc" desde **"Inicio → Ejecutar…"**) y compruebe el tipo de inicio de los servicios que se indican a continuación.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Administración de máquinas virtuales de Hyper-V	vmms	Automático	Configurado	
Agente de host NC	nchostagent	Deshabilitado	Configurado	
Aislamiento de claves CNG	keyiso	Automático	Configurado	
Instantáneas de volumen	vss	Manual	Configurado	
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado	
Servicio de cierre de invitado de Hyper-V	vmicshutdown	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio de intercambio de datos de Hyper-V		vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V		vmicheartbeat	Manual	Configurado	
Servicio de proceso de host de Hyper-V		vmcompute	Manual	Configurado	
Servicio de proxy DNS		DNSProxy	Deshabilitado	Configurado	
Servicio de red de host		hns	Manual	Configurado	
Servicio de sincronización de hora de Hyper-V		vmictimesync	Manual	Configurado	
Servicio de virtualización de Escritorio remoto de Hyper-V		vmicrdv	Manual	Configurado	
Servicio PowerShell Direct de Hyper-V		vmicvmsession	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V		vmicvss	Manual	Configurado	
Software Load Balancer Host Agent		SlbHostAgent	Manual	Configurado	
11. Inicie la consola de PowerShell		Ejecute la consola de PowerShell. Para ello pulse sobre "Inicio", seleccione **"Windows Powershell → Windows Powershell"** con el botón derecho y pulse sobre la opción **"Más → Ejecutar como administrador"**. 			
12. Verifique que se están aplicando los objetos GPO necesarios		Verifique que se están aplicando las GPOs correspondientes ejecutando el comando "gpresult /r". 			

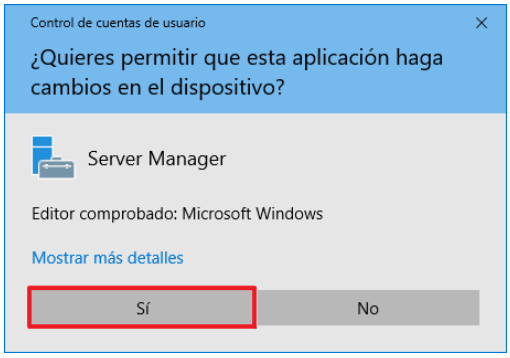
Comprobación	OK/NOK	Cómo hacerlo
13. Verifique que se están aplicando los objetos GPO necesarios		Verifique que se aplican los siguientes objetos GPO y en el siguiente orden. – CCN-STIC-578 ENS Incremental Servidor de Hyper-V Categoria alta - DL. – CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL. – CCN-STIC-570A ENS incremental Dominio categoria alta - DL. 
14. Verifique que la instalación se ha realizado correctamente		Utilizando la herramienta de administración de Hyper-V (ejecutando "virtmgmt.msc" desde **Inicio → Ejecutar…**), verifique que la consola se inicia y presenta el servidor local como un servidor de Hyper-V. 
15. Verifique que se disponen de conmutadores de red virtuales configurados		Utilizando la herramienta de administración de Hyper-V (ejecutando "virtmgmt.msc" desde **Inicio → Ejecutar…**), verifique haciendo uso de la opción "Administrador de conmutadores virtuales" del panel de acciones, que existen conmutadores virtuales configurados. 

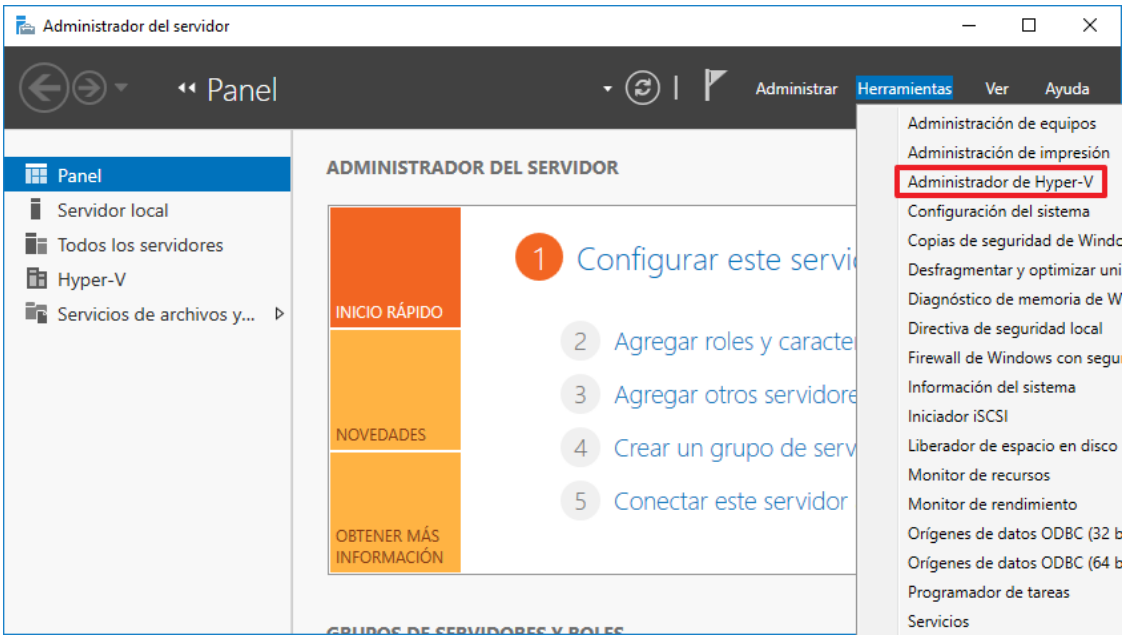
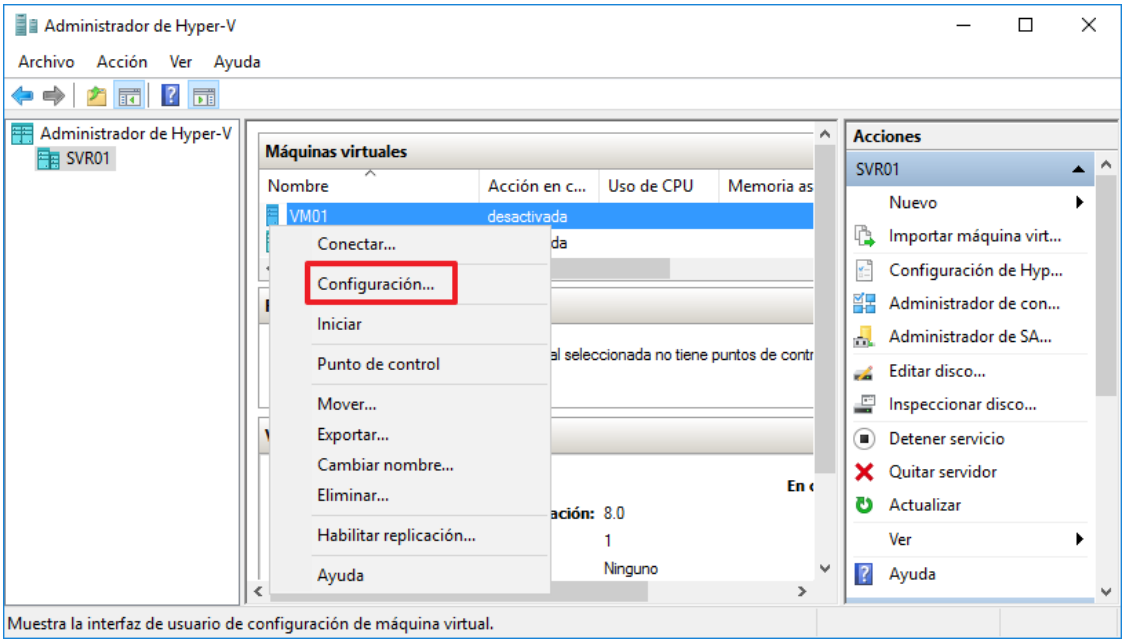
Comprobación	OK/NOK	Cómo hacerlo
16. Verifique que existen máquinas y que su configuración es adecuada		Utilizando la herramienta de administración de Hyper-V (ejecutando "virtmgmt.msc" desde **Inicio → Ejecutar…**), verifique que existen máquinas virtuales y que estas poseen la configuración adecuada haciendo clic derecho sobre cada una de ellas y seleccionando la opción del menú contextual "Configuración". 
17. Verifique la configuración de los adaptadores de red permiten la segregación de las máquinas virtuales		Utilizando la herramienta de administración de Hyper-V (ejecutando "virtmgmt.msc" desde **Inicio → Ejecutar…**), verifique en la configuración de cada máquina virtual que el conmutador virtual es el correcto.
18. Verifique que la auditoría sobre el servidor de Hyper-V se encuentra activada		Utilizando la herramienta de visor de eventos de Windows (ejecutando "eventvwr.msc" desde **Inicio → Ejecutar…**), verifique que la auditoría del servidor de Hyper-V se encuentra activada en todos sus componentes haciendo clic derecho sobre cada uno de sus registros. 

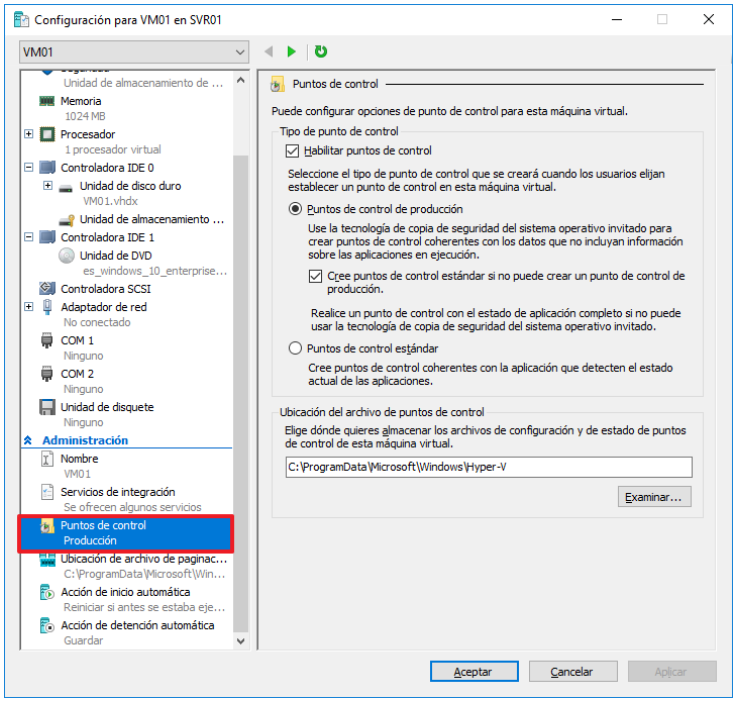
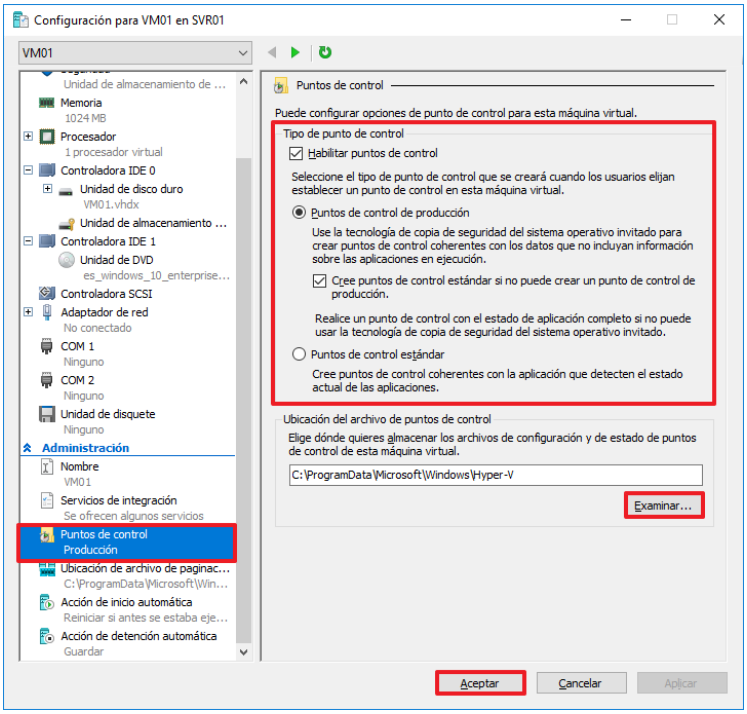
ANEXO A.5. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD

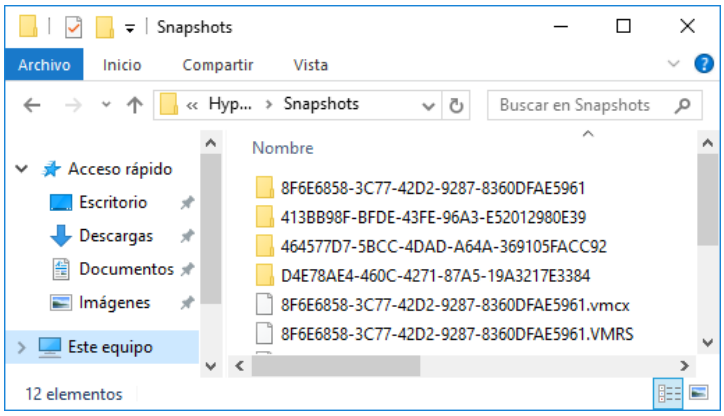
ANEXO A.5.1. GESTIÓN DE PUNTOS DE CONTROL DE MÁQUINAS VIRTUALES

1. GESTIÓN Y ALMACENAMIENTO DE PUNTOS DE CONTROL

Paso	Descripción
1.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
2.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
3.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar.  **Nota:** Dependiendo de la categoría definida en su organización es posible que se pidan credenciales de administrador para completar la acción.

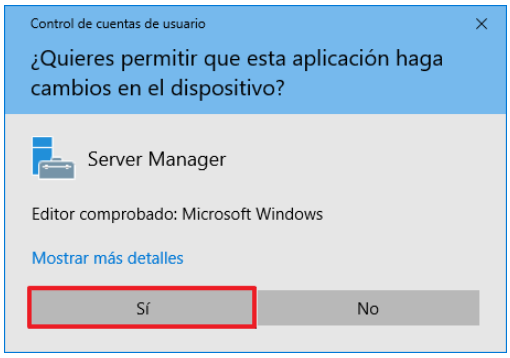
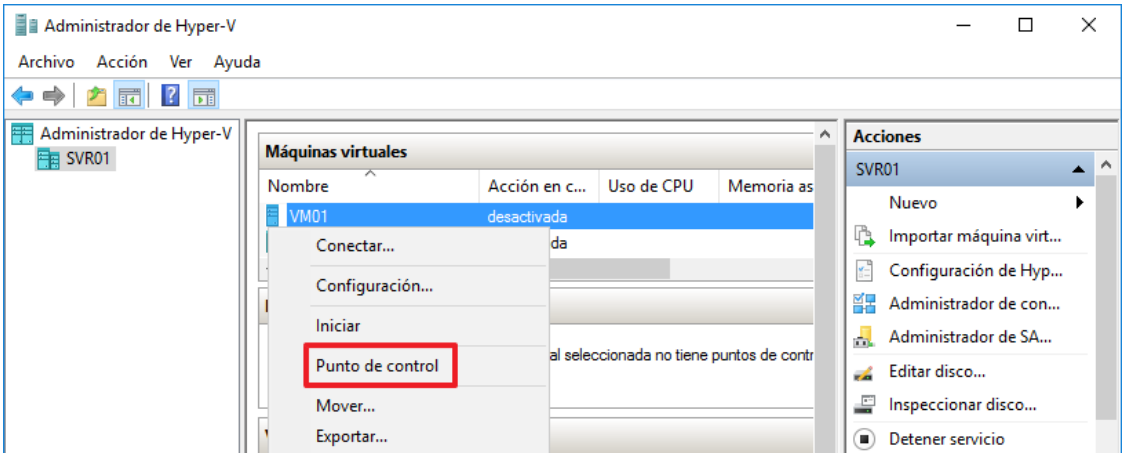
Paso	Descripción
4.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
5.	Seleccione con el botón derecho la máquina sobre la que desea administrar los puntos de control y pulse sobre la opción del menú contextual "Configuración…". 

Paso	Descripción
6.	En la ventana emergente sitúese sobre la sección “Administración” y a continuación sobre el apartado “Puntos de control”. 
7.	Evalúe la configuración de tipo de punto de control y seleccione la ubicación deseada para dichos puntos de control haciendo uso del botón “Examinar…”. Pulse “Aceptar” cuando haya finalizado.  **Nota:** Si la máquina virtual ya dispone de puntos de control no podrá modificar la ruta por defecto donde se ubican, debido a la pérdida de integridad que podrían sufrir dichos puntos de control.

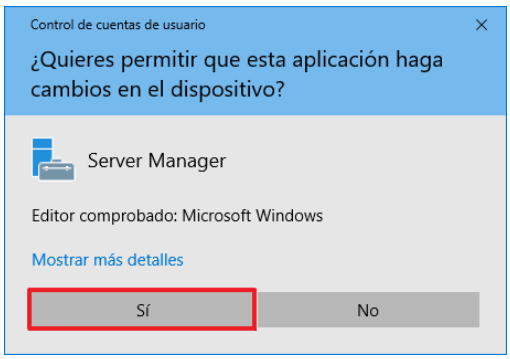
Paso	Descripción
8.	Dentro del directorio indicado existirán ficheros correspondientes a los puntos de control de cada máquina si todas poseen el mismo directorio o de una máquina virtual concreta si dispone de un directorio dedicado.  **Nota:** En este ejemplo se utiliza el directorio por defecto. Adapte estos pasos a las necesidades de su organización.

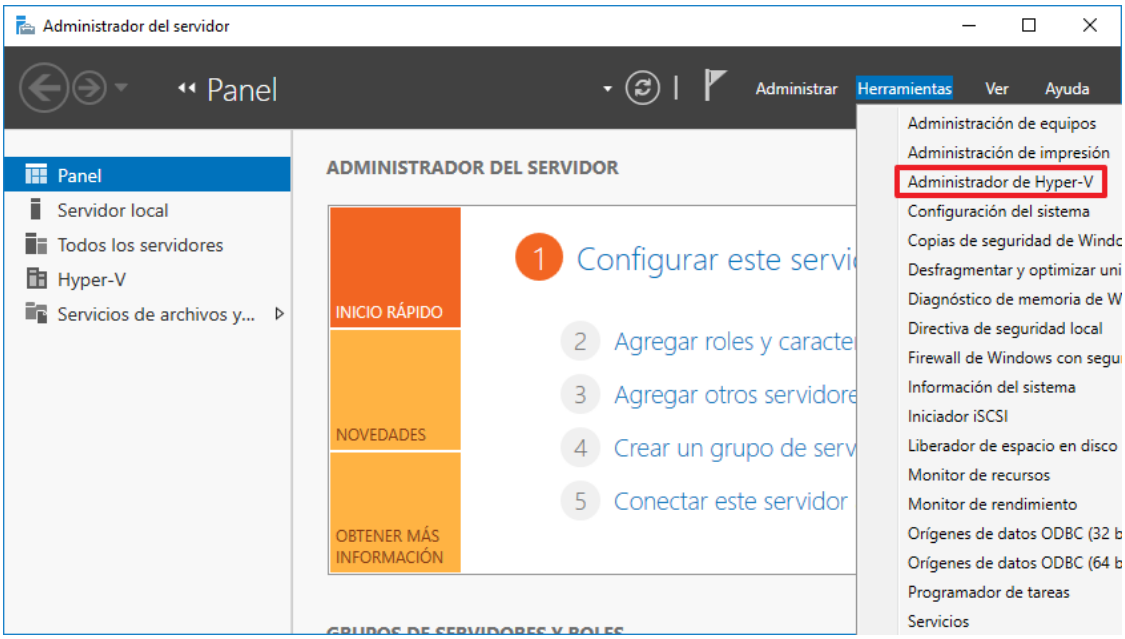
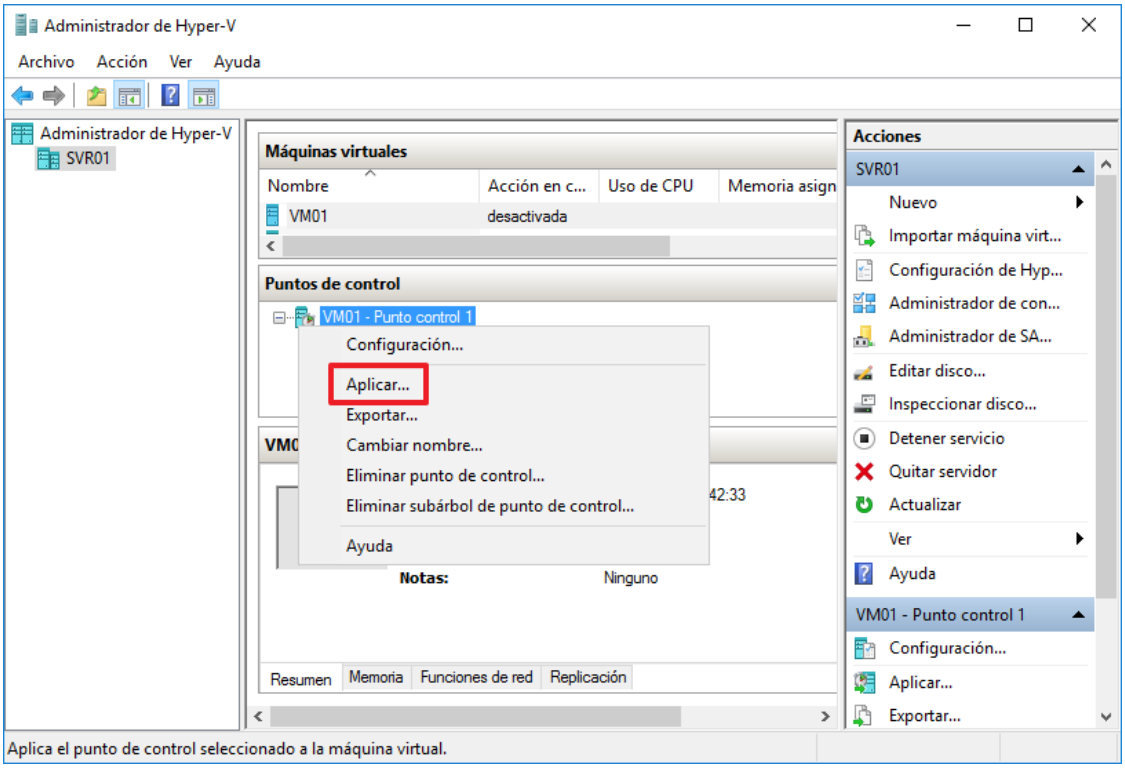
2. CREACIÓN DE PUNTOS DE CONTROL

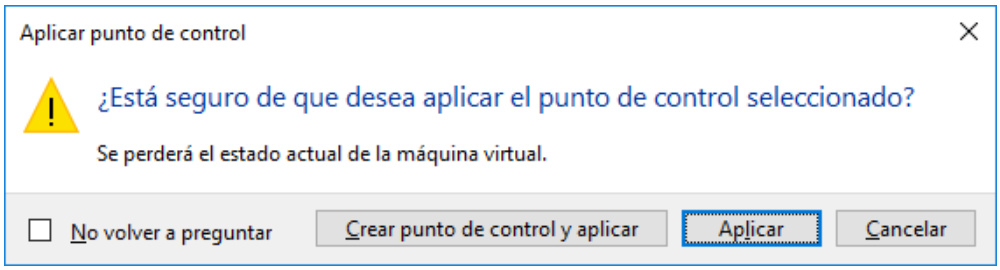
Paso	Descripción
9.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
10.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 

Paso	Descripción
11.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar.  **Nota:** Dependiendo de la categoría definida en su organización es posible que se pidan credenciales de administrador para completar la acción.
12.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
13.	Seleccione la máquina deseada con el botón derecho y pulse sobre la opción del menú contextual "Punto de control". 
14.	A partir de este momento se dispondrá de un punto de control que puede ser utilizado para recuperar el estado en el que se tomó la instantánea.

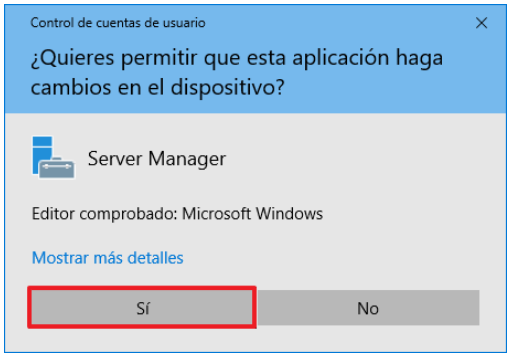
3. RECUPERACIÓN DE PUNTOS DE CONTROL

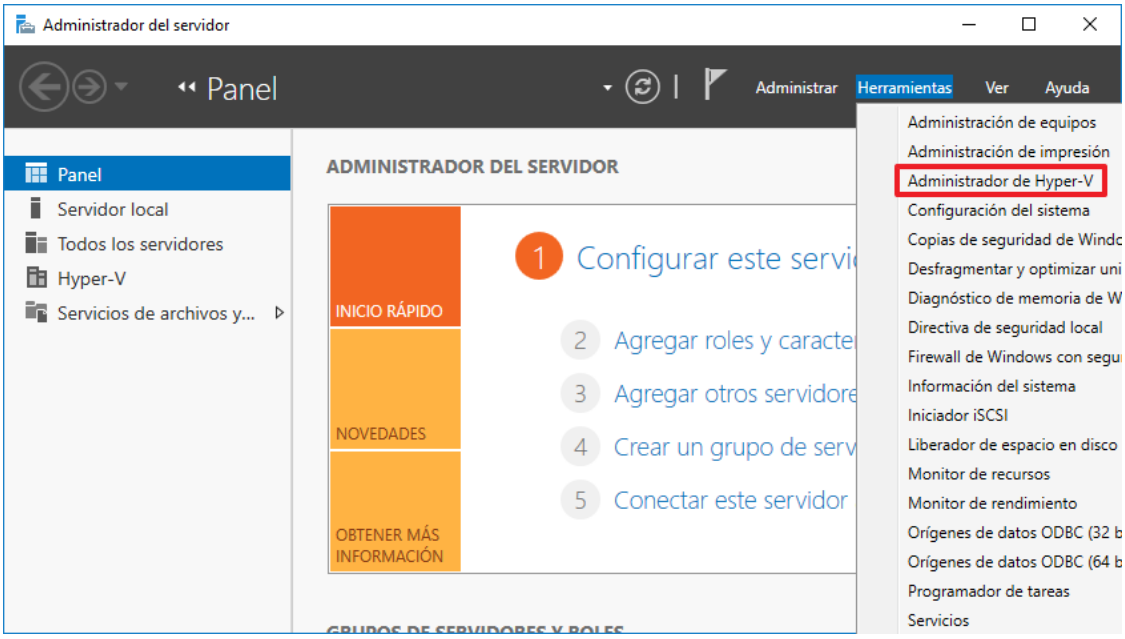
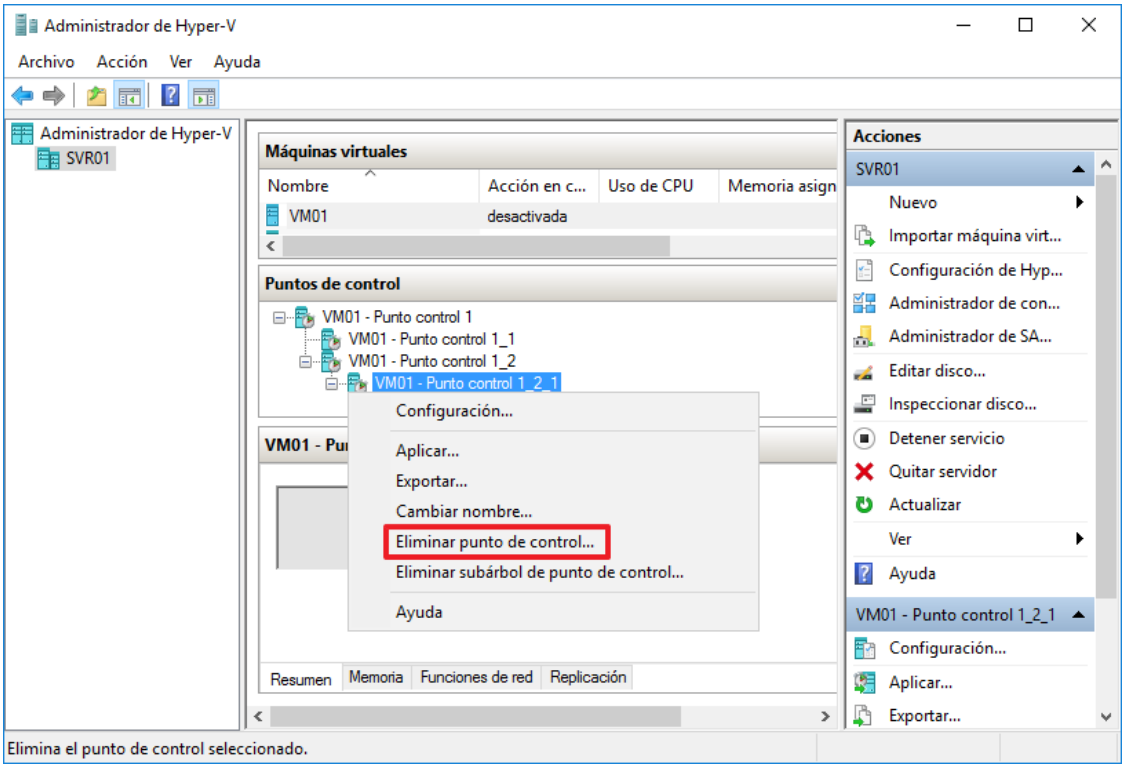
Paso	Descripción
15.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
16.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
17.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar.  **Nota:** Dependiendo de la categoría definida en su organización es posible que se pidan credenciales de administrador para completar la acción.

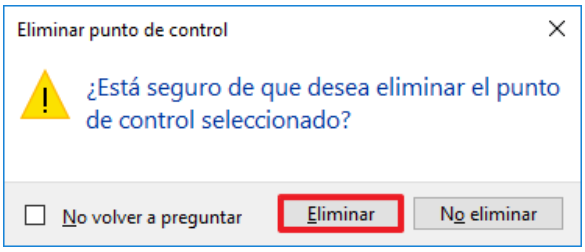
Paso	Descripción
18.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
19.	Seleccione la máquina virtual deseada y dentro de la sección "Puntos de control", seleccione el punto de control requerido con el botón derecho y seleccione la opción del menú contextual "Aplicar…". 

Paso	Descripción
20.	Ante el mensaje de advertencia pulse sobre la acción necesaria.  **Nota:** En este ejemplo se hace uso de la opción "Aplicar" ya que no es necesario crear otro punto de control adicional.
21.	El proceso de aplicación del punto de control comenzará.

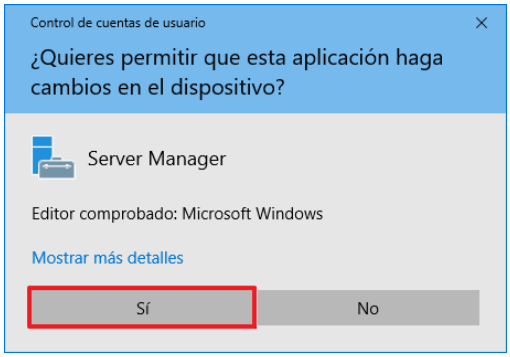
4. ELIMINACIÓN DE PUNTOS DE CONTROL

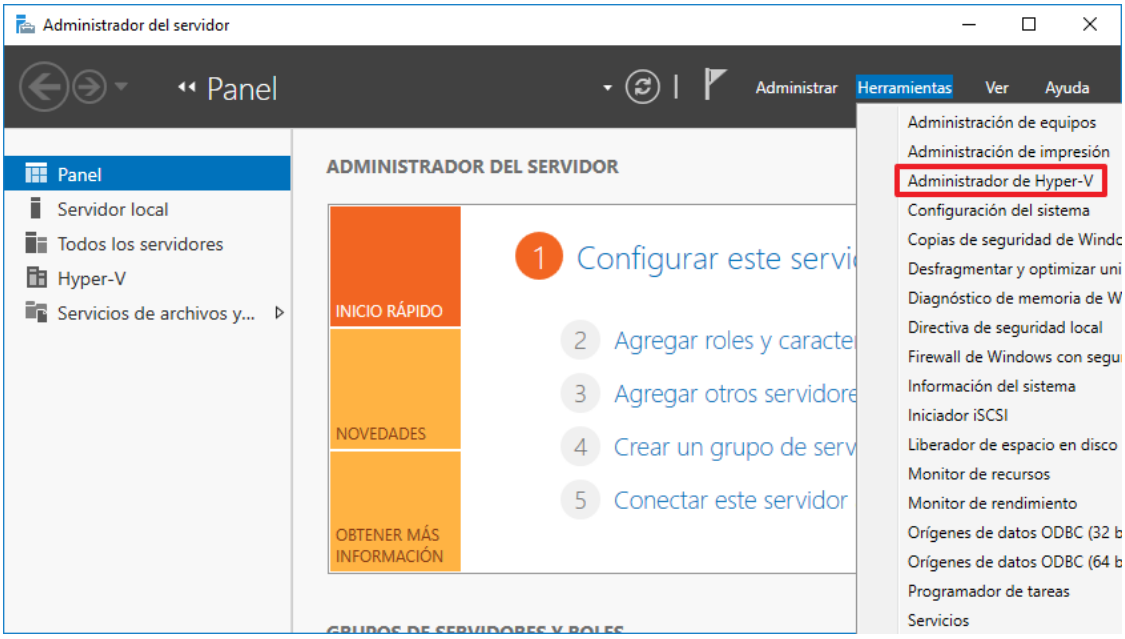
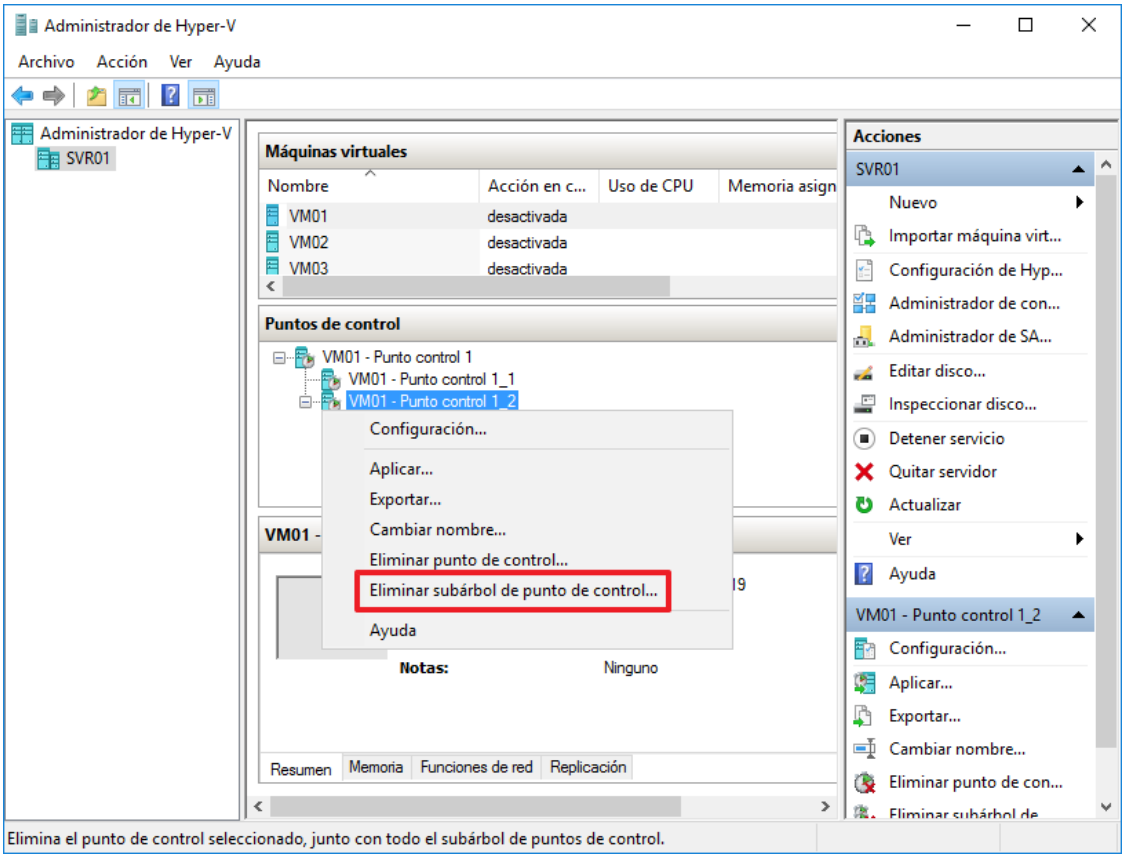
Paso	Descripción
22.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
23.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas.
24.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar.  **Nota:** Dependiendo de la categoría definida en su organización es posible que se pidan credenciales de administrador para completar la acción.

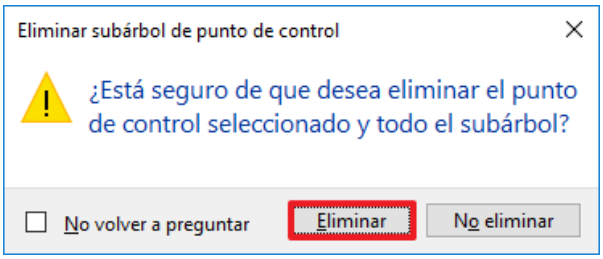
Paso	Descripción
25.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
26.	Seleccione la máquina virtual deseada y dentro de la sección "Puntos de control", seleccione el punto de control requerido con el botón derecho y seleccione la opción del menú contextual "Eliminar punto de control". 

Paso	Descripción
27.	Ante el mensaje de advertencia pulse sobre “Eliminar”. 
28.	Comenzará el proceso de eliminación del punto de control.

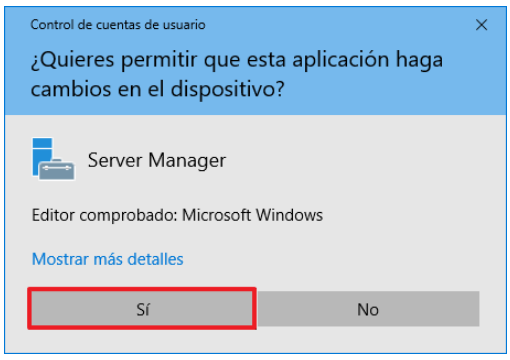
5. ELIMINACIÓN DE ÁRBOLES DE PUNTOS DE CONTROL

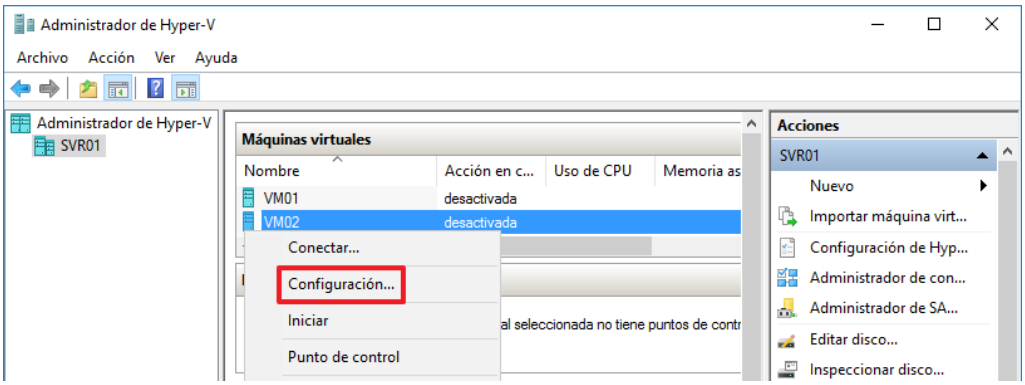
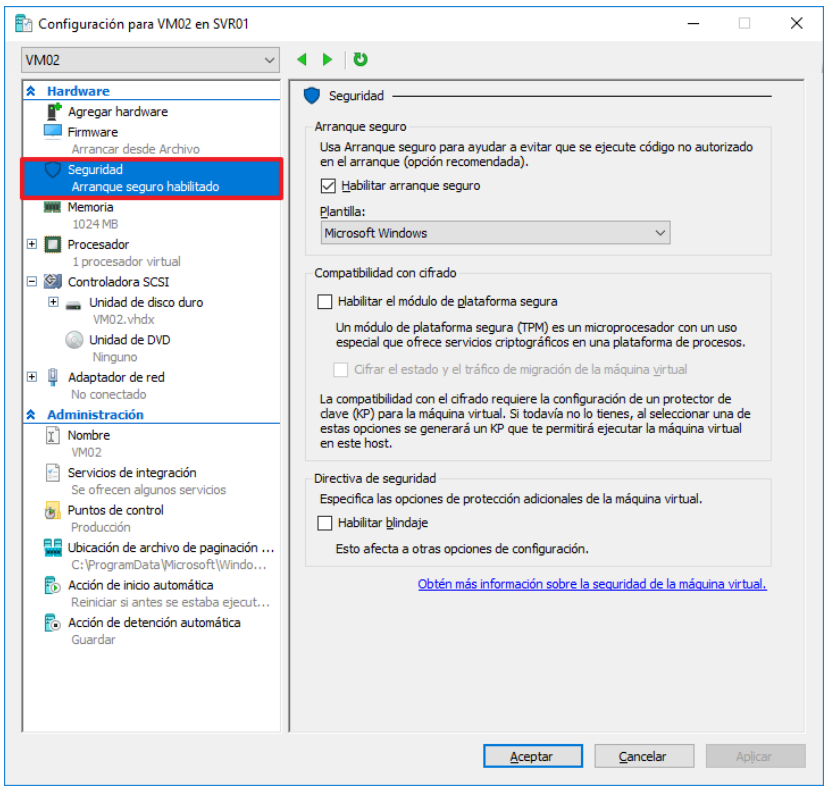
Paso	Descripción
29.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
30.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
31.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.  **Nota:** Dependiendo de la categoría definida en su organización es posible que se pidan credenciales de administrador para completar la acción.

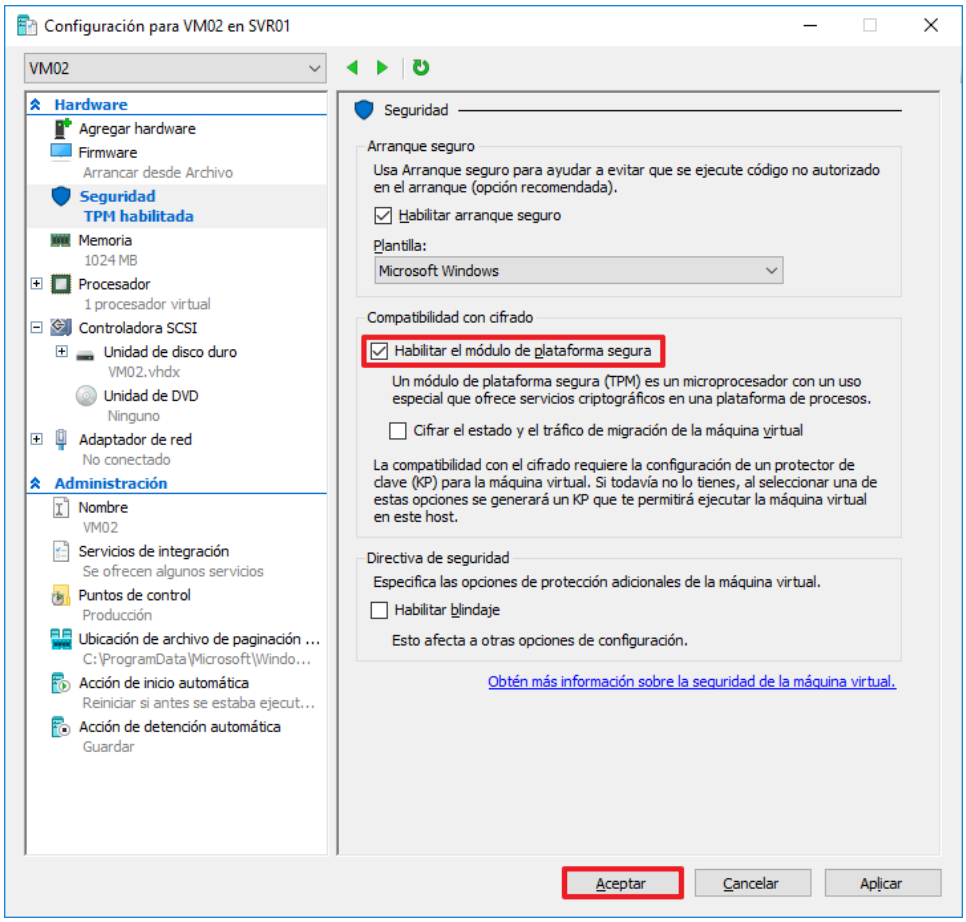
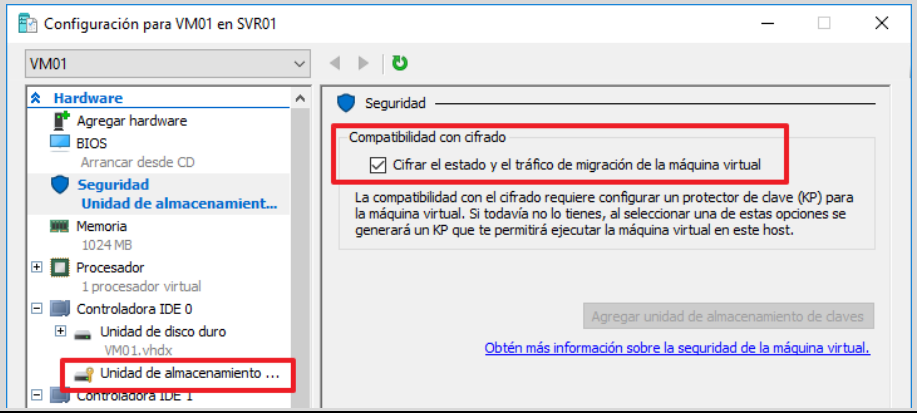
Paso	Descripción
32.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
33.	Seleccione la máquina virtual deseada y dentro de la sección "Puntos de control", seleccione el punto de control requerido con el botón derecho y seleccione la opción del menú contextual "Eliminar subárbol de punto de control…". 

Paso	Descripción
34.	Ante el mensaje de advertencia pulse sobre “Eliminar”. 
35.	Comenzará el proceso de eliminación del punto de control y todos los puntos de control que dependieran de dicho punto de control.

ANEXO A.5.2. CIFRADO DE MÁQUINAS VIRTUALES

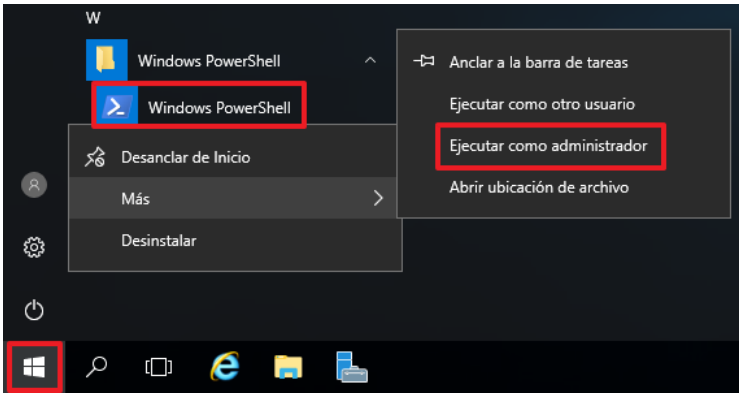
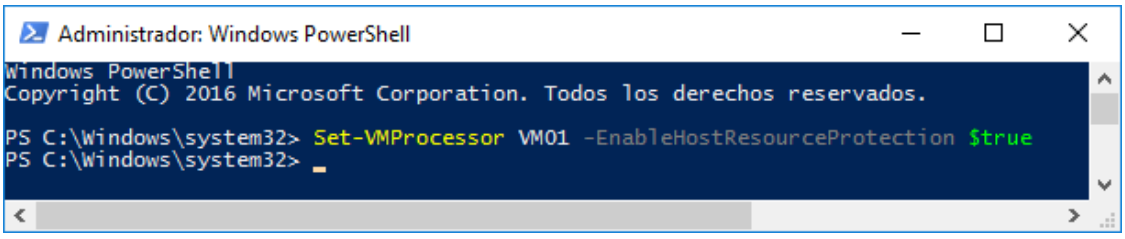
Paso	Descripción
36.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
37.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
38.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 

Paso	Descripción
39.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
40.	Seleccione la máquina deseada con el botón derecho y pulse sobre la opción del menú contextual "Configuración…". 
41.	Seleccione dentro del aparatado "Hardware" en el panel izquierdo, la opción "Seguridad". 

Paso	Descripción
42.	Marque la opción “Habilitar el módulo de plataforma segura” y pulse “Aceptar”.  **Nota:** Esta configuración solo será posible con máquinas que hayan sido configuradas como “Generación 2”. Es posible hacer uso de la configuración “Cifrar el estado y el tráfico de migración de la máquina virtual” tanto en la generación 2 como en la 1. Para esta última será necesario configurar una “Unidad de almacenamiento de claves”. 
43.	A partir de este momento dentro de la máquina virtual podrá hacer uso de la funcionalidad BitLocker para cifrar la máquina virtual.

ANEXO A.5.3. PROTECCIÓN DE RECURSOS OTORGADOS POR HYPER-V

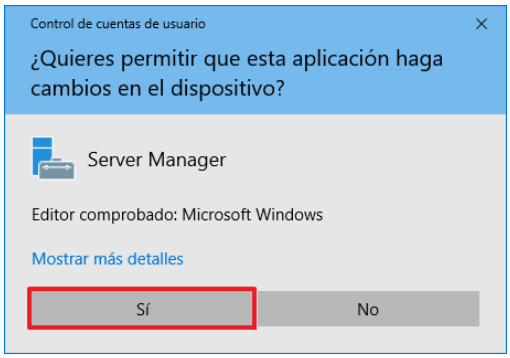
Esta característica ayuda a evitar que una máquina virtual use más recursos de los que le han sido asignados buscando niveles de actividad excesivos. Esto puede ayudar a evitar que la actividad excesiva de una máquina virtual degrade el rendimiento del propio Hyper-V o de otras máquinas virtuales albergadas en éste.

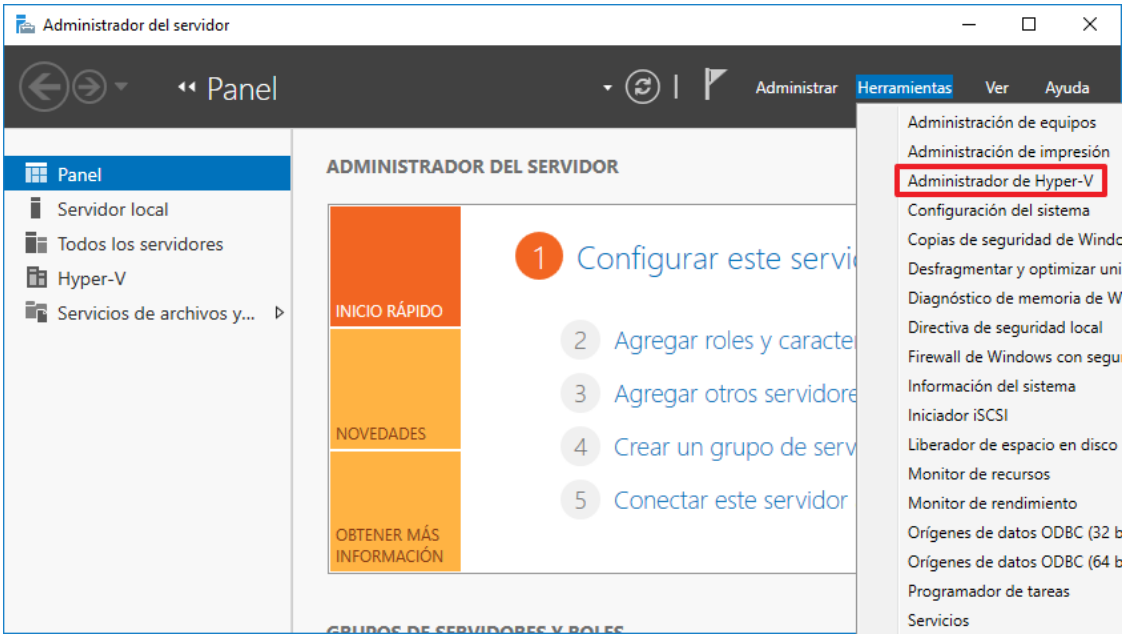
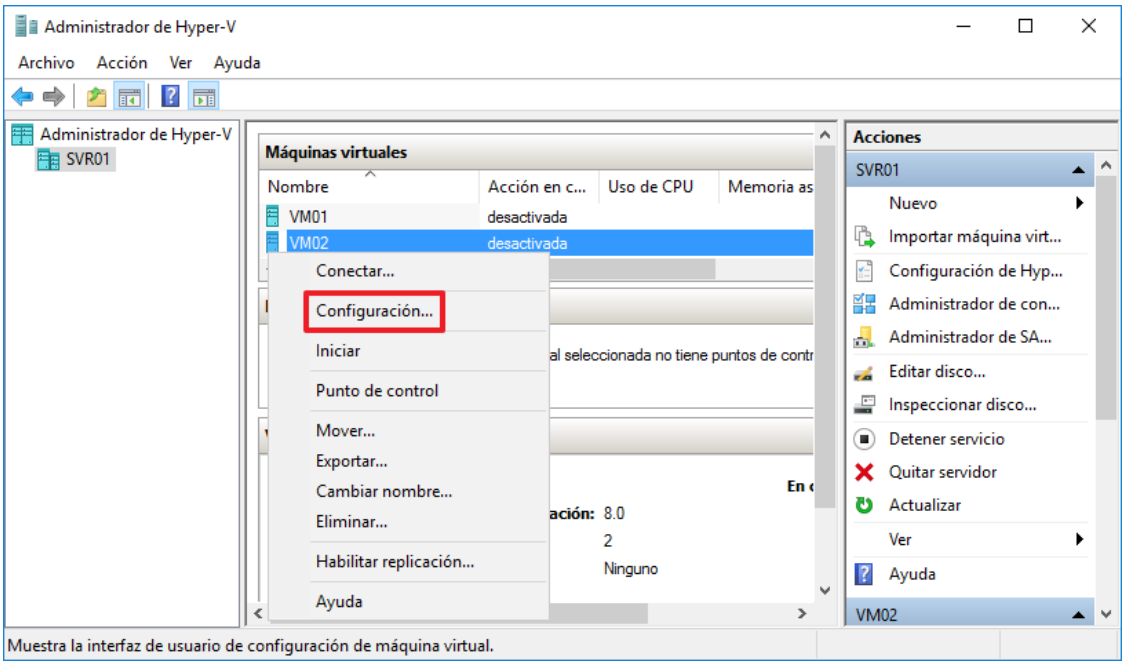
Paso	Descripción
44.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
45.	Inicie la consola de PowerShell. Para ello pulse sobre "Inicio", seleccione **"Windows Powershell → Windows Powershell"** con el botón derecho y pulse sobre la opción **"Más → Ejecutar como administrador"**. 
46.	Ejecute el siguiente comando: **Set-VMProcessor [Nombre_Maquina_Virtual] -EnableHostResourceProtection $true** 

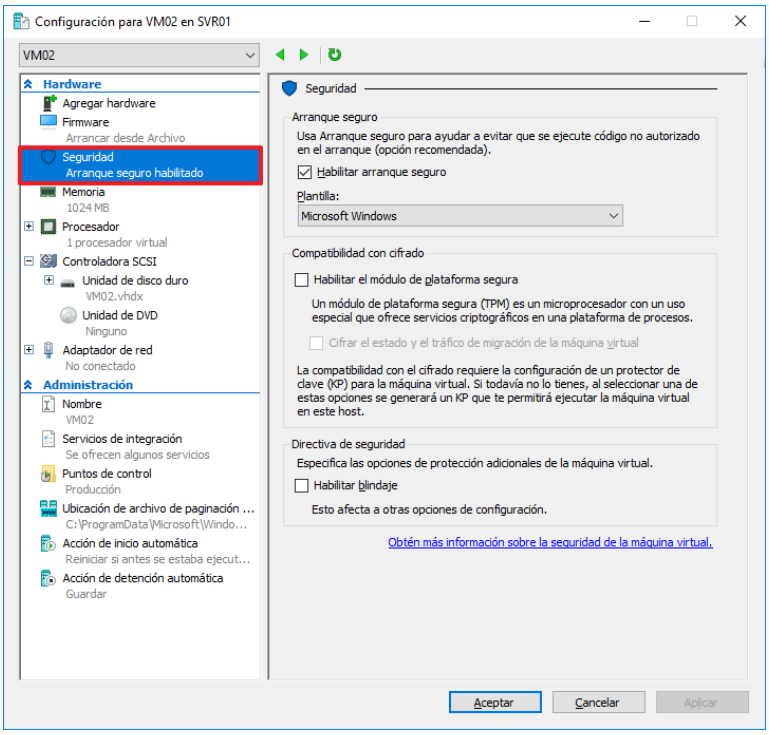
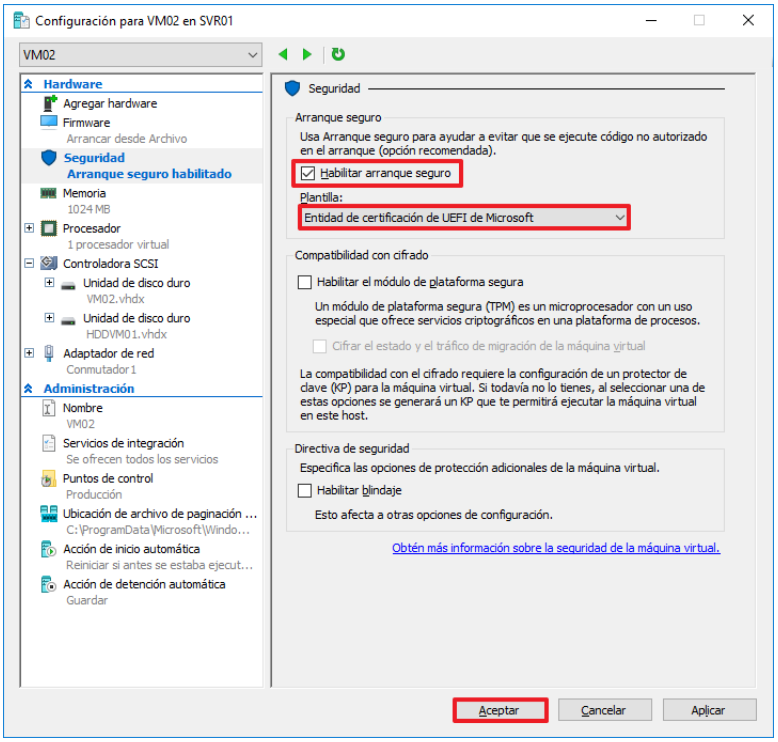
ANEXO A.5.4. ARRANQUE SEGURO PARA SISTEMAS OPERATIVOS

Todas las máquinas de "Generación 2" disponen de la opción de "Arranque seguro" habilitada en su configuración de seguridad. Los sistemas Windows poseen la configuración predefinida para este tipo de arranque, sin embargo, los sistemas operativos Linux no disponían de esta configuración hasta ahora.

Los sistemas operativos Ubuntu 14.04 y versiones posteriores, SUSE Linux Enterprise Server 12 y versiones posteriores, Red Hat Enterprise Linux 7.0 y versiones posteriores, y CentOS 7.0 y versiones posteriores están habilitados para el inicio seguro en servidores que ejecutan Windows Server 2016.

Paso	Descripción
47.	Inicie sesión en el equipo miembro del dominio donde se va aplicar seguridad para el Servidor de Hyper-V según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
48.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
49.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar.  **Nota:** Dependiendo de la categoría definida en su organización es posible que se pidan credenciales de administrador para completar la acción.

Paso	Descripción
50.	Inicie la herramienta "Administrador de Hyper-V". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administrador de Hyper-V"**. 
51.	Seleccione la máquina deseada con el botón derecho y pulse sobre la opción del menú contextual "Configuración…". 

Paso	Descripción
52.	Seleccione dentro del aparatado “Hardware” en el panel izquierdo, la opción “Seguridad”. 
53.	A continuación, en el panel derecho marque dentro de “Arranque seguro” la opción “Habilitar arranque seguro”, si no lo estuviese y la opción de “Plantilla:” denominada “Entidad de certificación de UEFI de Microsoft”.  **Nota:** Deberá realizar esta configuración antes de ejecutar la máquina virtual.