centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 575

IMPLEMENTACIÓN DEL ENS EN MICROSOFT SQL SERVER 2016 SOBRE MICROSOFT WINDOWS SERVER 2016

MAYO 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

NIPO: 083-19-179-3

Fecha de Edición: mayo de 2019
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

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

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

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

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

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

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

mayo de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE SQL SERVER 2016 EN EL ENS 8

ANEXO A.1. CONFIGURACIÓN SEGURA DE SQL SERVER 2016 SOBRE UN SERVIDOR MIEMBRO DE DOMINIO CON SISTEMA OPERATIVO WINDOWS SERVER 2016 . 9

1. APLICACIÓN DE MEDIDAS EN SQL SERVER 2016 9

1.1. MARCO ORGANIZATIVO 10

1.1.1. CONTROL DE ACCESO 10

1.1.1.1. OP. ACC. 2. REQUISITOS DE ACCESO 10

1.1.1.2. OP. ACC. 3. SEGREGACIÓN DE FUNCIONES Y TAREAS 11

1.1.1.3. OP. ACC. 4. PROCESO DE GESTIÓN DE DERECHOS DE ACCESO 12

1.1.1.4. OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN 13

1.1.1.5. OP. ACC. 6. ACCESO LOCAL 14

1.1.1.6. OP. ACC. 7. ACCESO REMOTO 14

1.1.2. EXPLOTACIÓN 15

1.1.2.1. OP. EXP. 1. INVENTARIO DE ACTIVOS 15

1.1.2.2. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD 15

1.1.2.3. OP. EXP. 3. GESTIÓN DE LA CONFIGURACIÓN 16

1.1.2.4. OP. EXP. 8. REGISTRO DE ACTIVIDAD DE LOS USUARIOS 16

1.2. MEDIDAS DE PROTECCIÓN 17

1.2.1. PROTECCIÓN DE LAS COMUNICACIONES 17

1.2.1.1. MP. COM. 3. PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD 17

1.2.2. PROTECCIÓN DE LA INFORMACIÓN 18

1.2.2.1. MP. INFO. 3. CIFRADO 18

1.2.2.2. MP. INFO. 9. COPIAS DE SEGURIDAD 18

2. RESUMEN Y APLICACIÓN DE MEDIDAS EN SQL SERVER 2016 19

ANEXO A.2. CATEGORÍA BÁSICA 21

ANEXO A.2.1. PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE MS SQL SERVER 2016 SOBRE SERVIDORES WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS 21

1. PREPARACIÓN DEL DOMINIO 21

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN 33

2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN 33

2.2. APLICACIÓN DE ESTÁNDARES INTERNACIONALES DE SEGURIDAD 38

2.3. GESTIÓN DE BASES DE DATOS 41

2.3.1. CREACIÓN DE BASES DE DATOS 41

2.3.2. MODIFICACIÓN DE BASES DE DATOS 46

2.3.3. ELIMINACIÓN DE BASES DE DATOS 49

2.4. GESTIÓN DE TABLAS 51

2.4.1. CREACIÓN DE TABLAS 51

2.4.2. MODIFICACIÓN DE TABLAS 54
2.4.3. ELIMINACIÓN DE TABLAS 56
2.4.4. INSERCIÓN DE DATOS 58
2.4.5. MODIFICACIÓN DE DATOS 60
2.4.6. ELIMINACIÓN DE DATOS 62
2.5. ASIGNACIÓN DE PERMISOS SOBRE SQL 64
2.5.1. PERMISOS EN BASES DE DATOS 64
2.5.2. PERMISOS DE USUARIOS SOBRE BASES DE DATOS 67
2.5.3. PERMISOS EN TABLAS 69
2.6. AUDITORÍA EN SQL SERVER 2016 73
2.7. SEGURIDAD SOBRE EL USUARIO SA 76
ANEXO A.2.2. LISTA DE COMPROBACIÓN DE SQL SERVER 2016 SOBRE WINDOWS SERVER 2016 PARA SERVIDORES QUE LES SON DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS 79
1. COMPROBACIONES EN CONTROLADOR DE DOMINIO 79
2. COMPROBACIONES EN EL SERVIDOR SQL SERVER 2016 82
ANEXO A.3. CATEGORÍA MEDIA 86
ANEXO A.3.1. PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE MS SQL SERVER 2016 SOBRE SERVIDORES WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS 86
1. PREPARACIÓN DEL DOMINIO 87
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN 97
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN 97
2.2. APLICACIÓN DE ESTÁNDARES INTERNACIONALES DE SEGURIDAD 102
2.3. GESTIÓN DE BASES DE DATOS 105
2.3.1. CREACIÓN DE BASES DE DATOS 105
2.3.2. MODIFICACIÓN DE BASES DE DATOS 108
2.3.3. ELIMINACIÓN DE BASES DE DATOS 111
2.4. GESTIÓN DE TABLAS 114
2.4.1. CREACIÓN DE TABLAS 114
2.4.2. MODIFICACIÓN DE TABLAS 117
2.4.3. ELIMINACIÓN DE TABLAS 119
2.4.4. INSERCIÓN DE DATOS 120
2.4.5. MODIFICACIÓN DE DATOS 122
2.4.6. ELIMINACIÓN DE DATOS 123
2.5. ASIGNACIÓN DE PERMISOS SOBRE SQL 125
2.5.1. PERMISOS EN BASES DE DATOS 125
2.5.2. PERMISOS DE USUARIOS SOBRE BASES DE DATOS 126
2.5.3. PERMISOS EN TABLAS 128
2.6. SEGREGACIÓN DE ROLES 133

2.7. SEGURIDAD SOBRE EL USUARIO SA 139
2.8. AUDITORÍA EN SQL SERVER 2016 142
ANEXO A.3.2. LISTA DE COMPROBACIÓN DE SQL SERVER 2016 SOBRE WINDOWS SERVER 2016 PARA SERVIDORES QUE LES SON DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS 145
1. COMPROBACIONES EN CONTROLADOR DE DOMINIO 145
2. COMPROBACIONES EN EL SERVIDOR SQL SERVER 2016 149
ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA 155
ANEXO A.4.1. PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE MS SQL SERVER 2016 SOBRE SERVIDORES WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA DEL ENS 155
1. PREPARACIÓN DEL DOMINIO 156
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN 166
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN 166
2.2. APLICACIÓN DE ESTÁNDARES INTERNACIONALES DE SEGURIDAD 170
2.3. GESTIÓN DE BASES DE DATOS 174
2.3.1. CREACIÓN DE BASES DE DATOS 174
2.3.2. MODIFICACIÓN DE BASES DE DATOS 178
2.3.3. ELIMINACIÓN DE BASES DE DATOS 180
2.4. GESTIÓN DE TABLAS 183
2.4.1. CREACIÓN DE TABLAS 183
2.4.2. MODIFICACIÓN DE TABLAS 186
2.4.3. ELIMINACIÓN DE TABLAS 188
2.4.4. INSERCIÓN DE DATOS 189
2.4.5. MODIFICACIÓN DE DATOS 190
2.4.6. ELIMINACIÓN DE DATOS 191
2.5. ASIGNACIÓN DE PERMISOS SOBRE SQL 193
2.5.1. PERMISOS EN BASES DE DATOS 193
2.5.2. PERMISOS DE USUARIOS SOBRE BASES DE DATOS 194
2.5.3. PERMISOS EN TABLAS 196
2.6. SEGREGACIÓN DE ROLES 200
2.7. SEGURIDAD SOBRE EL USUARIO SA 206
2.8. AUDITORÍA EN SQL SERVER 2016 208
2.9. MONITORIZACIÓN DE LA ACTIVIDAD DE SQL 213
2.10. CIFRADO DE CONEXIONES 216
2.10.1. CONFIGURACIÓN DEL CIFRADO SSL EN EL SERVIDOR DE SQL SERVER 216
ANEXO A.4.2. LISTA DE COMPROBACIÓN DE SQL SERVER 2016 SOBRE WINDOWS SERVER 2016 PARA SERVIDORES QUE LES SON DE APLICACIÓN LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA DEL ENS 222
1. COMPROBACIONES EN CONTROLADOR DE DOMINIO 222
2. COMPROBACIONES EN EL SERVIDOR SQL SERVER 2016 226

ANEXO A.5. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD 232
ANEXO A.5.1. ASIGNACIÓN DE PERMISOS SOBRE INTEGRATION SERVICES 232
ANEXO A.5.2. ASIGNACIÓN DE PERMISOS SOBRE REPORTING SERVICES 236
ANEXO A.5.3. ASIGNACIÓN DE PERMISOS SOBRE ANALYSIS SERVICES 240
ANEXO A.5.4. CIFRADO DE ELEMENTOS DE SQL SERVER 2016 244
ANEXO A.5.5. OCULTAR INSTANCIA DEL MOTOR DE BASE DE DATOS 248

ANEXO A. CONFIGURACIÓN SEGURA DE SQL SERVER 2016 EN EL ENS

Para los permisos asociados en el dominio de otros componentes de SQL Server cuya instalación es opcional revise los puntos de la presente guía referidos en el "ANEXO A.5 TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD". En el caso de que su organización necesite proporcionar servicios de Integration Services deberá aplicar el "ANEXO A.5.1 ASIGNACIÓN DE PERMISOS SOBRE INTEGRATION SERVICES". Si su organización debe proporcionar informes vía Reporting Services aplique a la configuración del dominio el "ANEXO A.5.2 ASIGNACIÓN DE PERMISOS SOBRE REPORTING SERVICES". En el caso de que su organización trabaje con servicios de Analysis Services en red deberá aplicar el "ANEXO A.5.3 ASIGNACIÓN DE PERMISOS SOBRE ANALYSIS SERVICES" de esta guía.

Deberá en función de la criticidad de la base de datos, tabla o campo endurecer y/o cifrar los objetos pertinentes se cara a proteger los datos y accesos a sus objetos específicos. Debe existir un análisis de riesgos y plan de contingencias acorde a su organización y negocio específico.

Deberá revisar que los permisos y seguridad aplicados a los objetos de su organización siguen vigentes y aplicándose con el transcurso del tiempo, sobre todo después de las distintas actualizaciones aplicadas en su organización.

Deberá revisar las posibles comunicaciones sobre seguridad de los productos pertenecientes a su organización.

En el caso de requerir procedimientos almacenados de sistema propios en su motor SQL Server, deberá aplicar los permisos más restrictivos a sus objetos y revisar que con las actualizaciones del motor siguen teniendo el comportamiento adecuado, sin menoscabo de revisar su seguridad después de cada actualización.

Recuerde revisar las recomendaciones de copias de seguridad y salvaguarda de las mismas en entornos físicamente distintos de su organización según las recomendaciones vigentes.

Revise la adecuación de todos los datos que almacenan sus bases de datos, asegúrese de que todos los datos que posee en sus bases de datos son explotados y deben estar en el motor.

Los planes de contingencia, pruebas de recuperación deben repetirse de manera cíclica.

Debe analizar el tipo y magnitud de crecimiento de sus bases de datos de cara a la anticipación de modificación y adquisición de recursos es su organización para que los motores de bases de datos puedan seguir prestando servicio. El número de accesos y rendimiento de servidores deben ser revisados periódicamente por la misma razón.

ANEXO A.1. CONFIGURACIÓN SEGURA DE SQL SERVER 2016 SOBRE UN SERVIDOR MIEMBRO DE DOMINIO CON SISTEMA OPERATIVO WINDOWS SERVER 2016

1. APLICACIÓN DE MEDIDAS EN SQL SERVER 2016

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación del Servidor de bases de datos SQL Server 2016 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 SQL Server 2016 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.

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 SQL Server 2016, así como otras medidas que puedan ser fácilmente aplicables mediante condiciones de seguridad válidas. Por ejemplo, todas aquellas medidas que puedan ser aplicadas a través de objetos de políticas de grupo (GPO) o las innatas a la gestión del sistema o al propio Directorio Activo, como la asignación de permisos para la segregación de roles y funciones.

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

Para un mejor entendimiento de las medidas 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 ORGANIZATIVO

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 bases de datos o el propio servidor que administra dichas bases de datos 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

Del mismo modo será necesario hacer uso de los propios mecanismos que implementa el servicio SQL Server 2016 para la asignación y revocación de permisos dentro de su propia estructura de bases de datos, pudiendo por ejemplo permitir o denegar el acceso de lectura sobre una base de datos completa o una tabla específica de dicha base de datos a un usuario perteneciente a la organización.

https://docs.microsoft.com/es-es/sql/relational-databases/security/permissions-database-engine?view=sql-server-2017

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.

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 SQL Server 2016. De este modo se evita modificar los permisos individuales de cada usuario para conceder o no permisos sobre un mismo recurso.

A través de los mecanismos que proporciona SQL Server 2016 es posible la creación de usuarios y grupos propios que permitan la administración y/o diversas tareas para usuarios que no pertenecen a la organización.

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 SQL Server 2016.

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. Este mismo ejemplo es aplicable a SQL Server 2016 ya que un usuario puede tener permisos de lectura sobre un conjunto de tablas, pero no por ello debe realizar una modificación de los datos que contiene.

Tal y como se citó en apartados anteriores SQL Server 2016 posee mecanismos para realizar la tarea de gestión de privilegios.

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 SQL Server 2016 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 SQL Server 2016 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 al propio sistema de bases de datos y los mecanismos que éste proporciona, y que por lo tanto deben establecerse.

Del mismo modo deberá tener en consideración la diferencia de un servicio de bases de datos SQL Server 2016 que soporta un entorno de producción y un servicio de bases de datos SQL Server 2016 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 SQL Server 2016 así como en el propio servicio de SQL Server 2016.

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

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

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

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

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

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 SQL Server 2016 deberá ser realizado de forma segura, así como el realizado a las bases de datos que este contiene siempre que la organización considere necesario y apruebe dicho privilegio. El método de conexión habitual entre los sistemas Windows para la conexión con bases de datos es "Microsoft Management Studio" 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 SQL Server 2016 está destinado al almacenamiento de bases de datos es necesario recopilar la información anteriormente requerida según el ENS. Por lo tanto, se requerirá conocer el número de bases de datos que contiene el servidor, la función de cada una y el responsable asociado a dicha base de datos.

1.1.2.2. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD

Se considera que el Servidor SQL Server 2016 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.

c) Eliminación de recursos de ejemplo.

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 los servicios que proporciona SQL Server 2016, limitando su funcionalidad a los servicios estrictamente necesarios para el desempeño de las tareas asignadas.

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 SQL Server 2016.

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 SQL Server 2016, implementa mecanismos para la auditoría de acceso a objetos y acciones realizadas dentro del propio servicio. 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 SQL Server 2016 mediante el empleo del firewall en su modalidad avanzada. Aunque se tratará en extensión en un anexo de la presente guía, el operador podrá conocer todos los detalles de esta solución a través de la información que proporciona el fabricante:

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

El servicio SQL Server 2016 implementa mecanismos de conexión segura contra el servidor, con el fin de proteger la integridad del mismo y permitiendo que el usuario que realiza la conexión sea quien dice ser.

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 SQL Server 2016 dispone de mecanismos que permiten realizar un cifrado de las bases de datos que este contiene. Esto es aplicable también a elementos más específicos de las bases de datos como tablas o columnas concretas.

1.2.2.2. MP. INFO. 9. COPIAS DE SEGURIDAD

Dentro del ENS, se 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 SQL Server 2016 posee mecanismos que permiten guardar y recuperar bases de datos completas o parciales con su correspondiente contenido.

2. RESUMEN Y APLICACIÓN DE MEDIDAS EN SQL SERVER 2016

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

Control	Medida	Mecanismo de aplicación
OP. ACC. 2	Requisitos de acceso	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-575, adaptándolos a la organización.
OP. ACC. 3	Segregación de funciones y tareas	Revisión e implementación de guía CCN-STIC-575, adaptándolos a la organización.
OP. ACC. 4	Proceso de gestión de derechos de acceso	Revisión e implementación de guía CCN-STIC-575, 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-575, 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-575, adaptándolos a la organización.
OP. EXP. 1	Inventario de activos	Revisión e implementación de guía CCN-STIC-575, adaptándolos a la organización.
OP. EXP. 2	Configuración de seguridad	Revisión e implementación de guía CCN-STIC-575, adaptándolos a la organización.
OP. EXP. 3	Gestión de la configuración	Revisión e implementación de guía CCN-STIC-575, adaptándolos a la organización.

Control	Medida	Mecanismo de aplicación
OP. EXP. 8	Registro de actividad de los usuarios	Revisión e implementación de guía CCN-STIC-575, 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-575, adaptándolos a la organización.
MP. INFO. 3	Cifrado	Revisión e implementación de guía CCN-STIC-575, adaptándolos a la organización.
MP. INFO. 9	Copias de seguridad	Revisión e implementación de guía CCN-STIC-575, adaptándolos a la organización.

ANEXO A.2. CATEGORÍA BÁSICA

ANEXO A.2.1. PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE MS SQL SERVER 2016 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 SQL Server 2016 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.

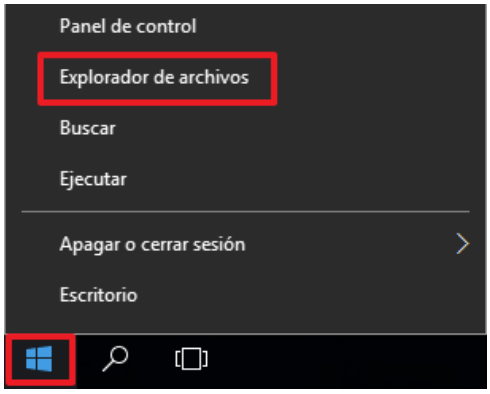
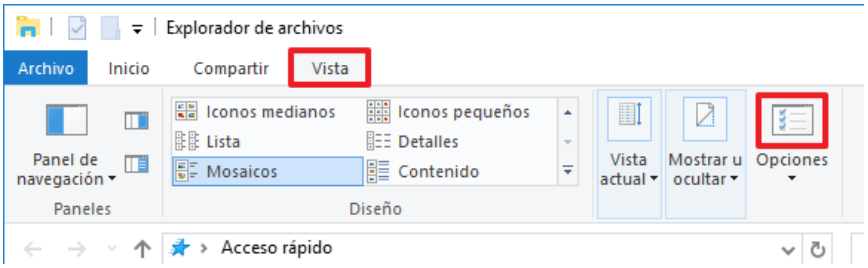
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

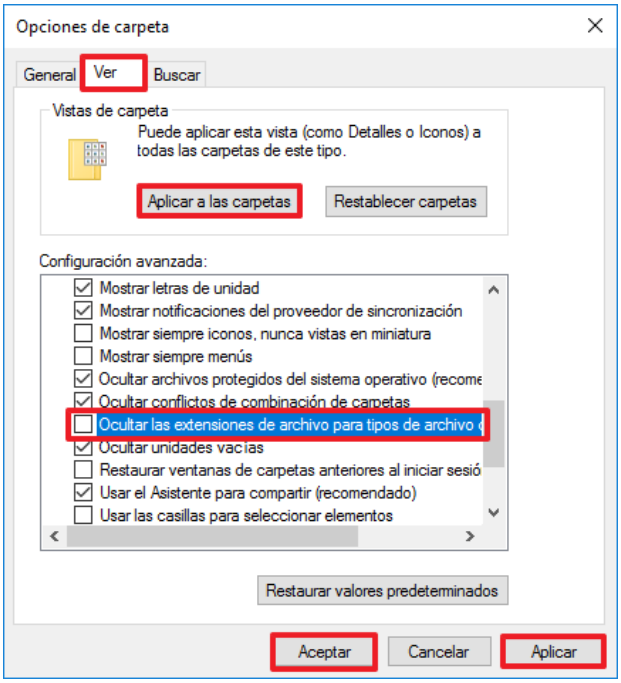
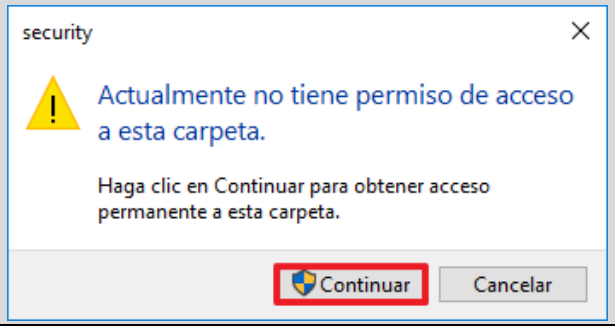
1. PREPARACIÓN DEL DOMINIO

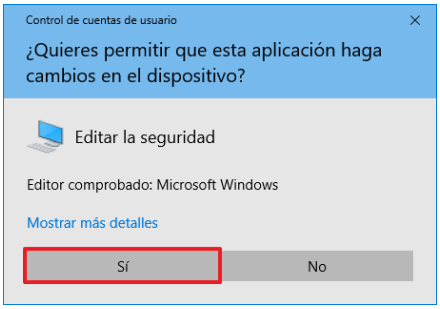
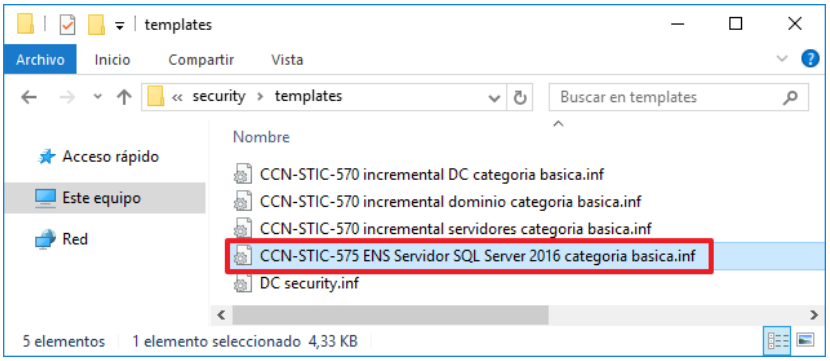
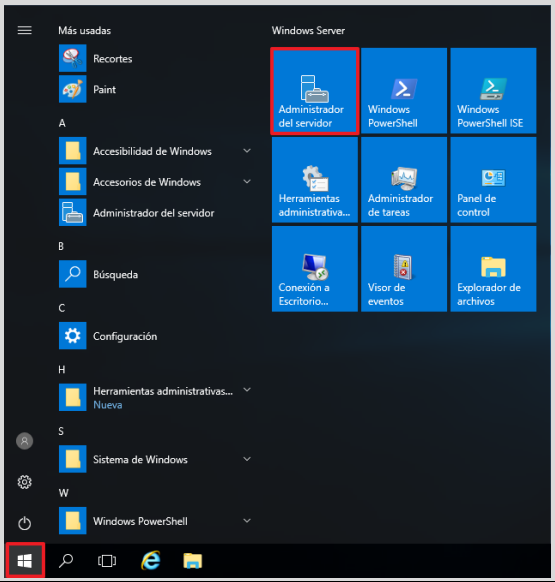
Los pasos que se describen a continuación deberá realizarlos en un Controlador de Dominio del dominio al que pertenece el equipo servidor que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer servidor de SQL Server 2016 que actúe como miembro del dominio. Durante este procedimiento se crea la unidad organizativa que contiene los servidores de SQL Server y se realizan las configuraciones de políticas de grupo correspondientes.

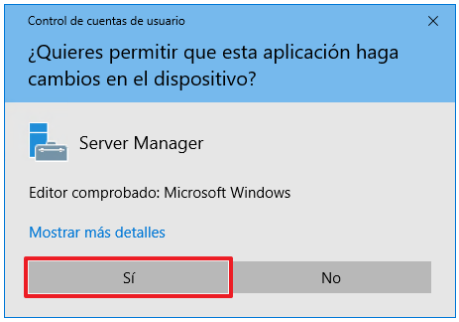
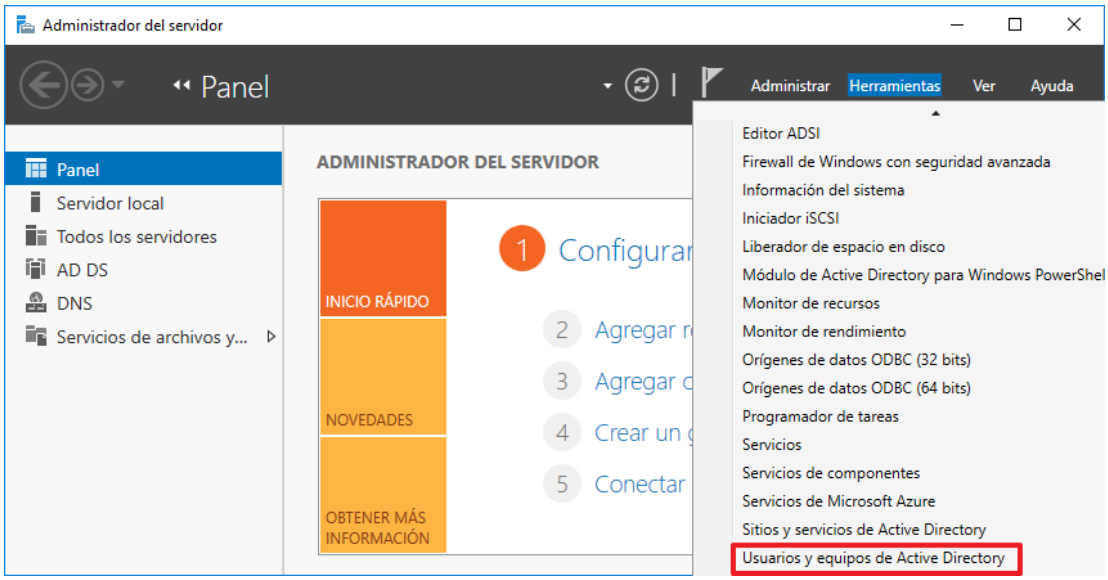
Nota: Esta guía asume que los servidores Controladores del Dominio al que pertenece el equipo servidor de SQL Server que está asegurando, se les ha aplicado la configuración descrita en la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016". Si no es así, aplique la guía correspondiente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

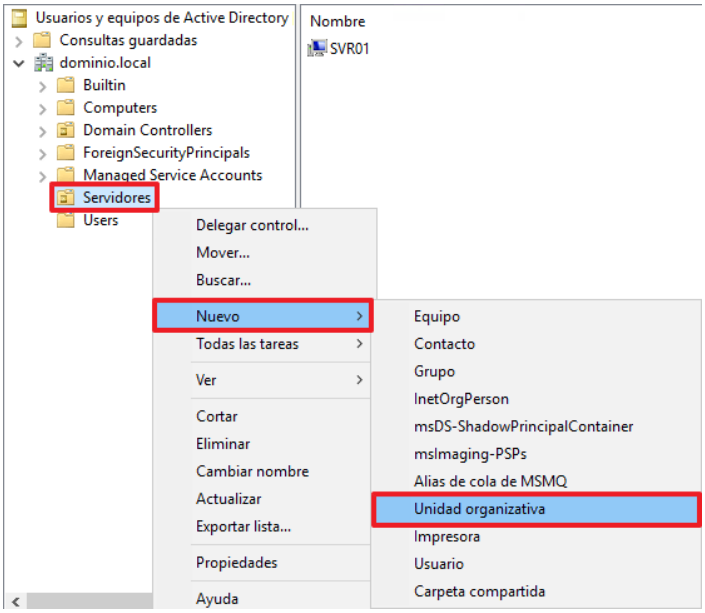
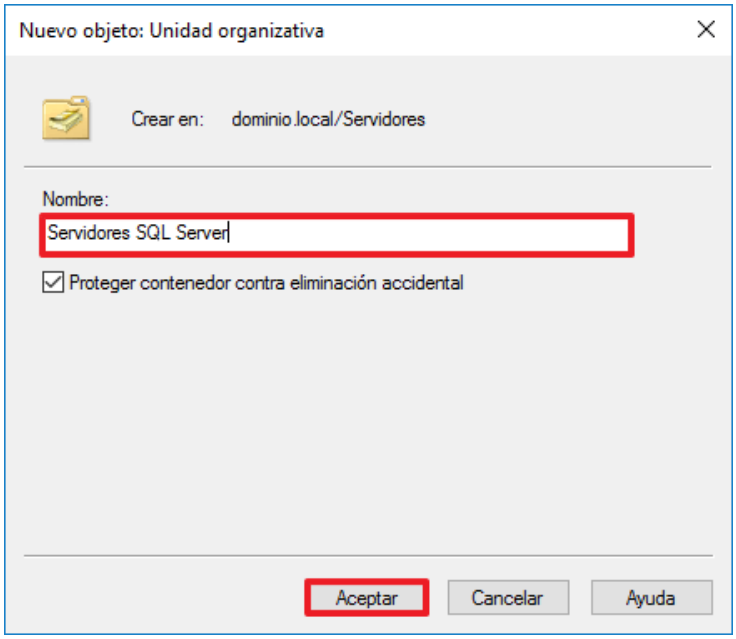
Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio del dominio donde se va a aplicar seguridad para el servidor SQL Server 2016 según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

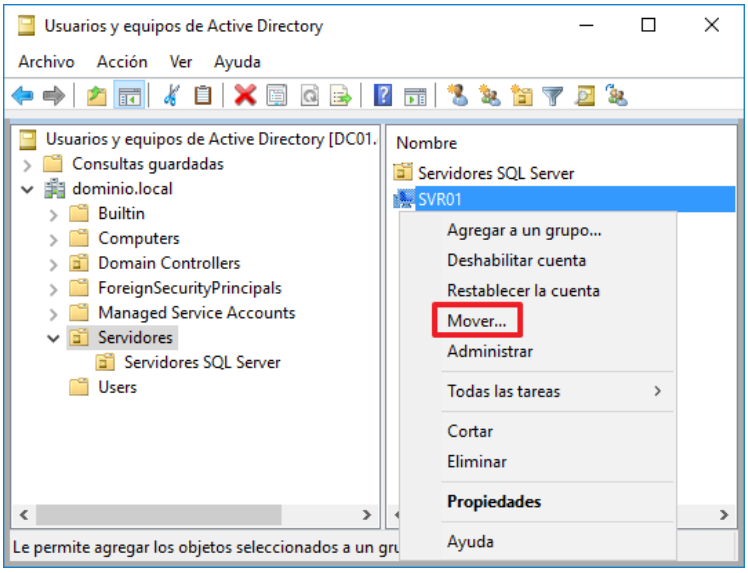
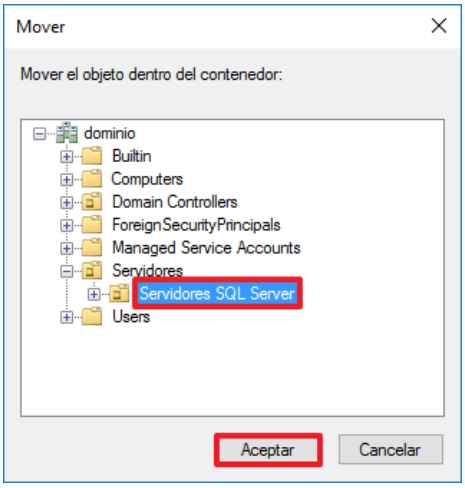
Paso	Descripción
2.	Cree el directorio "Scripts" en la unidad "C:\". **Nota:** Los scripts asumen que su ubicación en el sistema será bajo "C:\Scripts". Si los colocara en otra ubicación, tendrá que editar los scripts para reflejar la nueva ubicación.
3.	Copie los scripts y plantillas de seguridad asociadas 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. 
5.	En el "Explorador de archivos" pulse sobre la pestaña "Vista" del menú superior y seleccione el icono de "Opciones". 

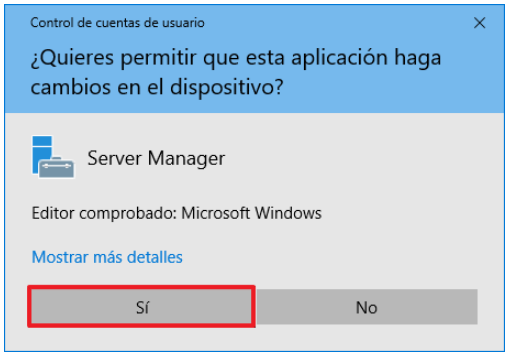
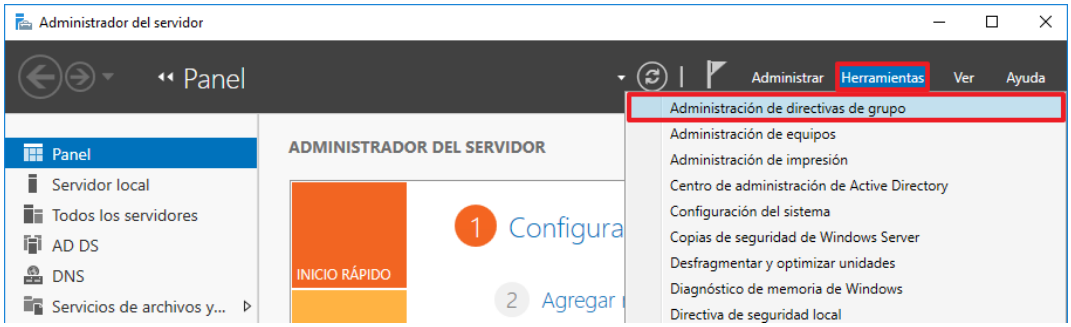
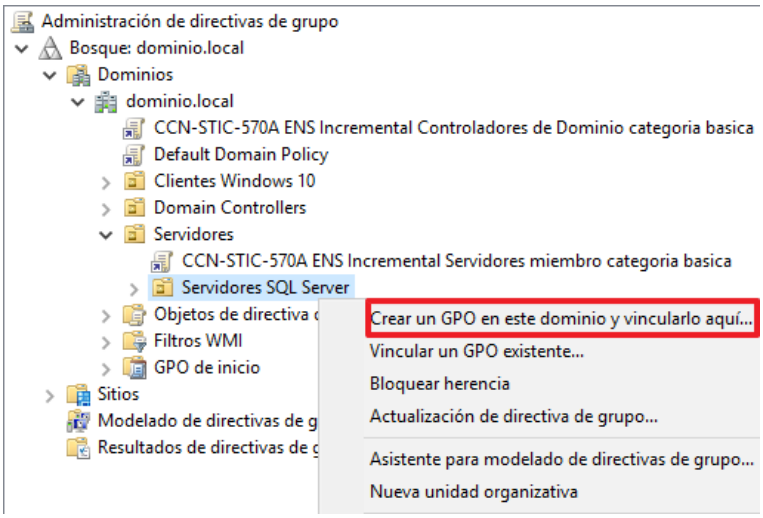
Paso	Descripción
6.	En "Opciones de carpeta" sitúese en la pestaña "Ver" y en el campo "Configuración avanzada" localice y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos". Pulse primero sobre el botón "Aplicar", después sobre "Aplicar a las carpetas" (Pulse "Sí" ante el mensaje de confirmación) y, por último, pulse "Aceptar". 
7.	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. 

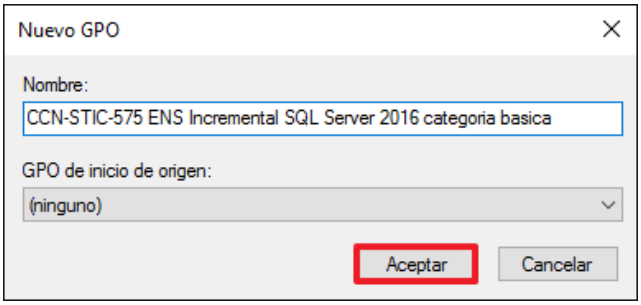
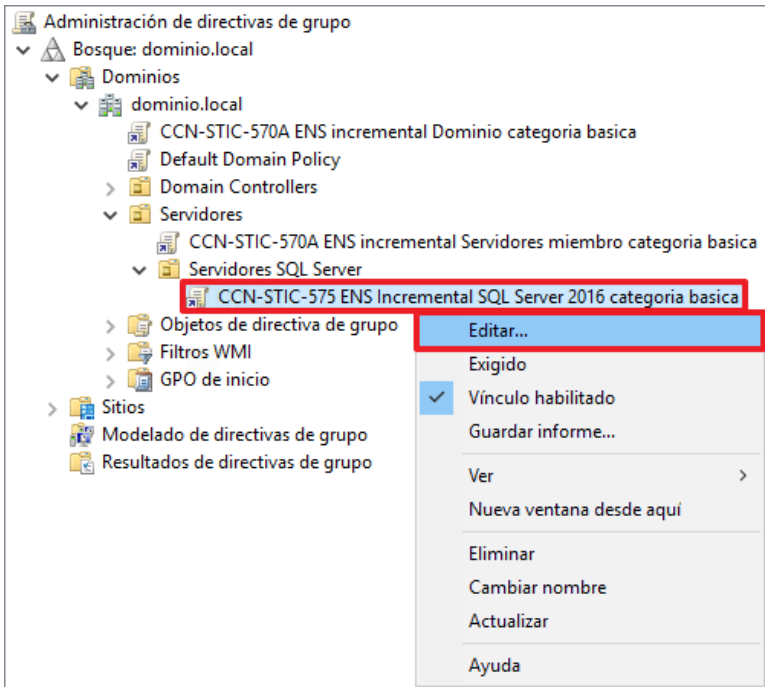
Paso	Descripción
8.	El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse "Sí" para continuar. 
9.	Copie el fichero "CCN-STIC-575 ENS Servidor SQL Server 2016 categoria basica.inf" al directorio "%SYSTEMROOT%\Security\Templates" del Controlador de Dominio. 
10.	A continuación, abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas.  **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"**. 

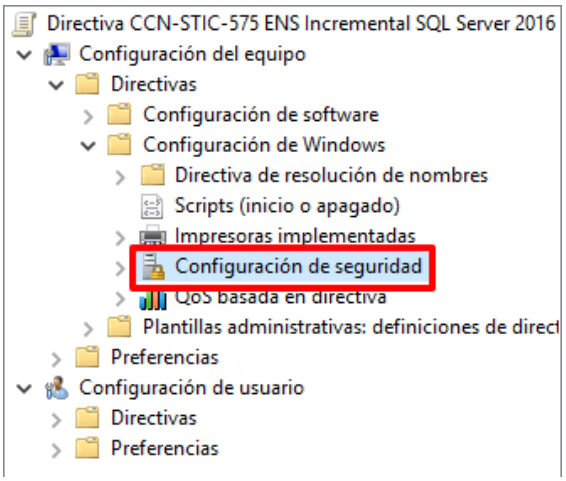
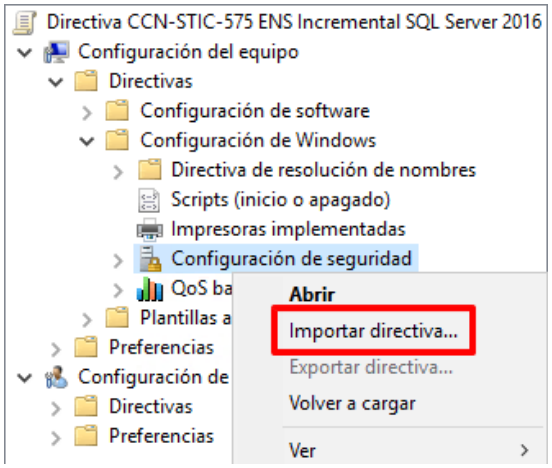
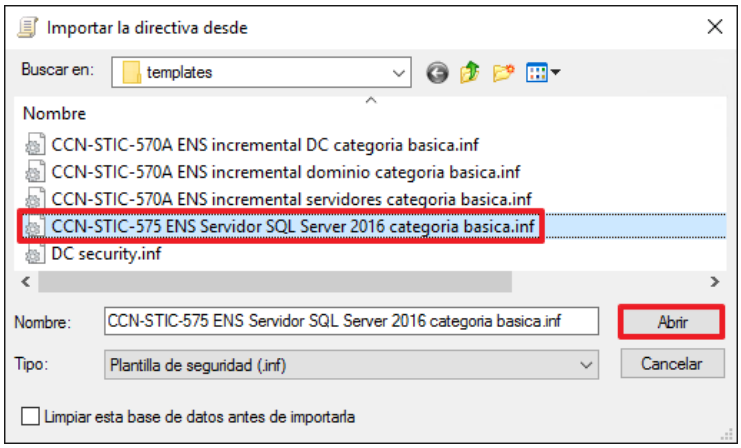
Paso	Descripción
11.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
12.	Inicie la herramienta de usuarios y equipos del Directorio Activo. Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione **"Herramientas → Usuarios y equipos de Active Directory"**. 

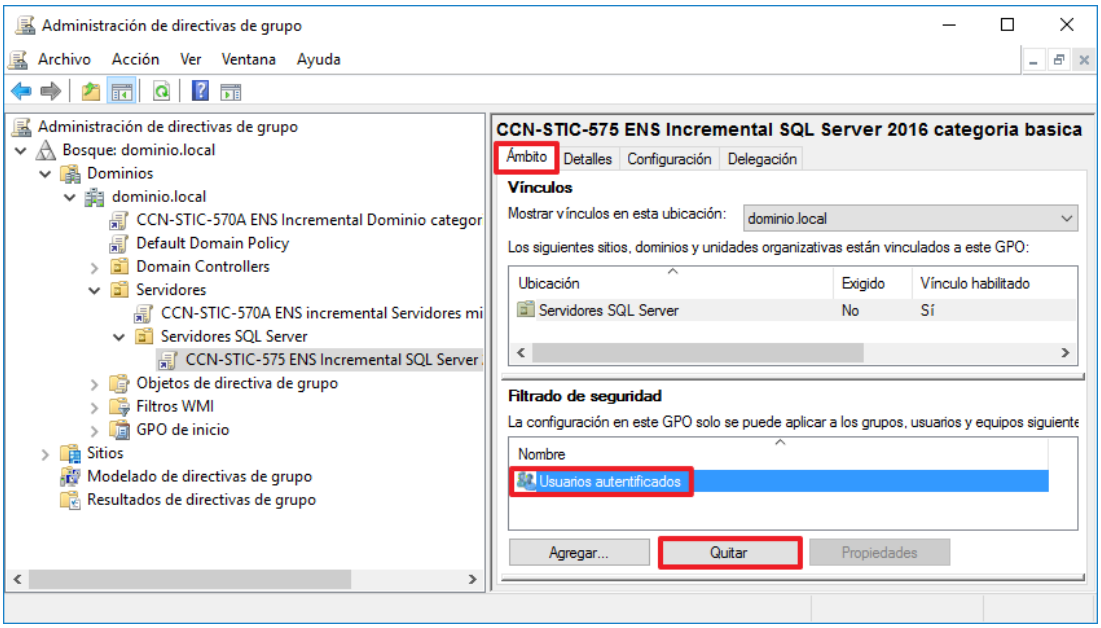
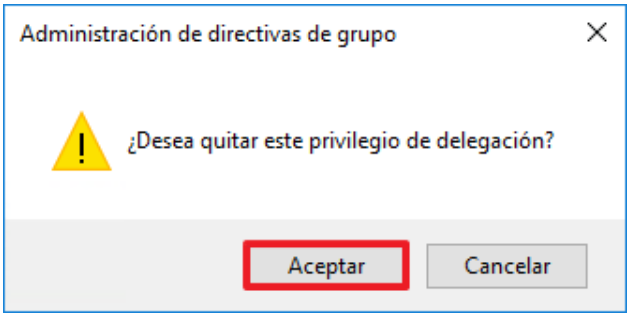
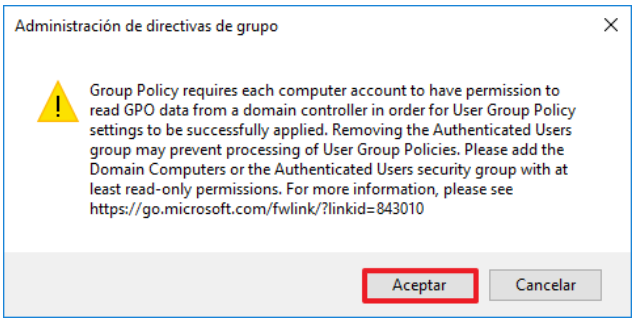
Paso	Descripción
13.	En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo **"<<dominio>> → <<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 **"dominio.local → Servidores"**.
14.	Introduzca el nombre "Servidores SQL Server" tal y como se muestra en la imagen y pulse sobre "Aceptar".  **Nota:** Puede establecer el nombre que más se adecúe a las necesidades de su organización.

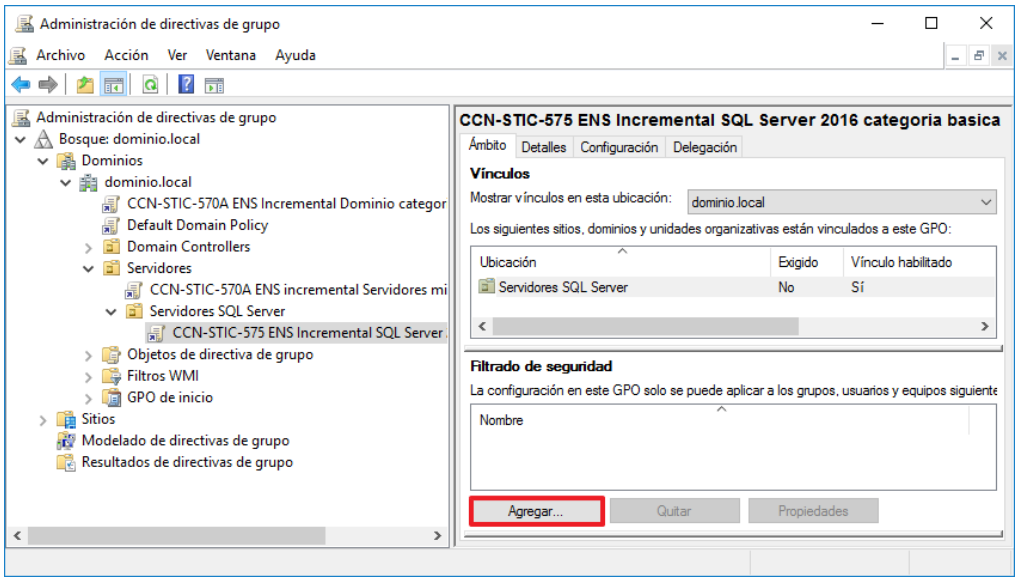
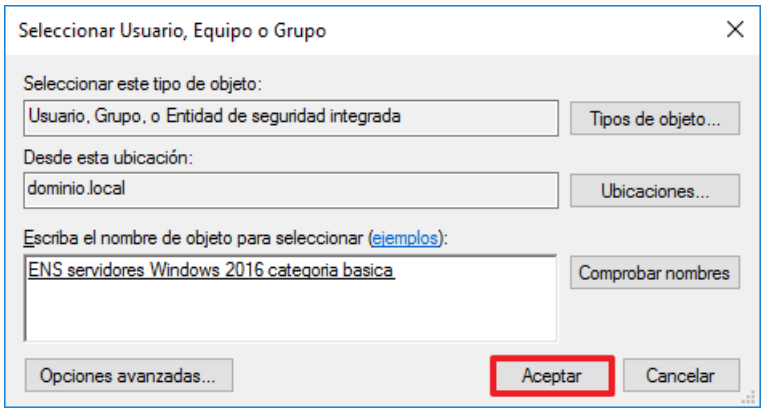
Paso	Descripción
15.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores de virtualización a la unidad organizativa "Servidores de SQL Server". Para ello, haga clic con el botón derecho sobre el equipo que desee reubicar y seleccione la opción del menú contextual "Mover...". 
16.	A continuación, seleccione la unidad organizativa "Servidores de SQL Server" y pulse sobre "Aceptar". 
17.	Cierre la herramienta "Usuarios y equipos de Active Directory".
18.	A continuación, deberá crear la GPO "CCN-STIC-575 ENS incremental Servidor de SQL Server categoria basica". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 

Paso	Descripción
19.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
20.	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".** 
21.	A continuación, despliegue el nodo **"Bosque: <<nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores SQL Server"**. **Nota:** En este ejemplo el nombre de la unidad organizativa donde se encuentran todos los servidores que implementan este rol, "Servidores SQL Server".
22.	Pulse con el botón derecho sobre la unidad organizativa "Servidores de SQL Server" y seleccione "Crear un GPO en este dominio y vincularlo aquí…". 

Paso	Descripción
23.	Introduzca el nombre del objeto GPO, "CCN-STIC-575 ENS Incremental SQL Server 2016 categoria basica" y haga clic en el botón "Aceptar". 
24.	Seleccione la directiva recién creada "CCN-STIC-575 ENS Incremental SQL Server 2016 categoria basica". Se mostrará una ventana de aviso de la Consola de administración de directivas de grupo, informando que los cambios realizados son globales para la GPO y estos afectarán a todas las ubicaciones en las que se vincule esta GPO. Pulse "Aceptar" en este mensaje y haga clic con el botón derecho sobre ella y seleccione la opción "Editar". 

Paso	Descripción
25.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad"**. 
26.	Pulse con el botón derecho sobre "Configuración de seguridad" y seleccione la opción "Importar directiva…". 
27.	Sitúese en la carpeta "%SYSTEMROOT%\Security\Templates" y seleccione el fichero denominado "CCN-STIC-575 ENS Servidor SQL Server 2016 categoria basica.inf", seguidamente pulse en el botón "Abrir". 

Paso	Descripción
28.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
29.	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". 
30.	Pulse "Aceptar" ante el mensaje emergente "¿Desea quitar este privilegio de delegación?". 
31.	Pulse de nuevo "Aceptar" ante el mensaje de advertencia emergente. 

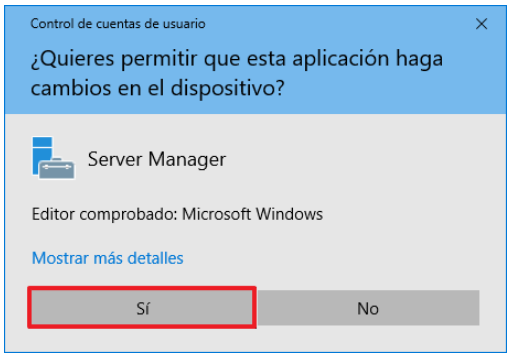
Paso	Descripción
32.	A continuación, pulse el botón "Agregar…".  **Nota:** En caso de no disponer del grupo mostrado, deberá adaptar estos pasos a las necesidades de su organización.
33.	Introduzca como nombre "ENS Servidores Windows 2016 categoria basica". Este grupo corresponde con el generado en la 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.

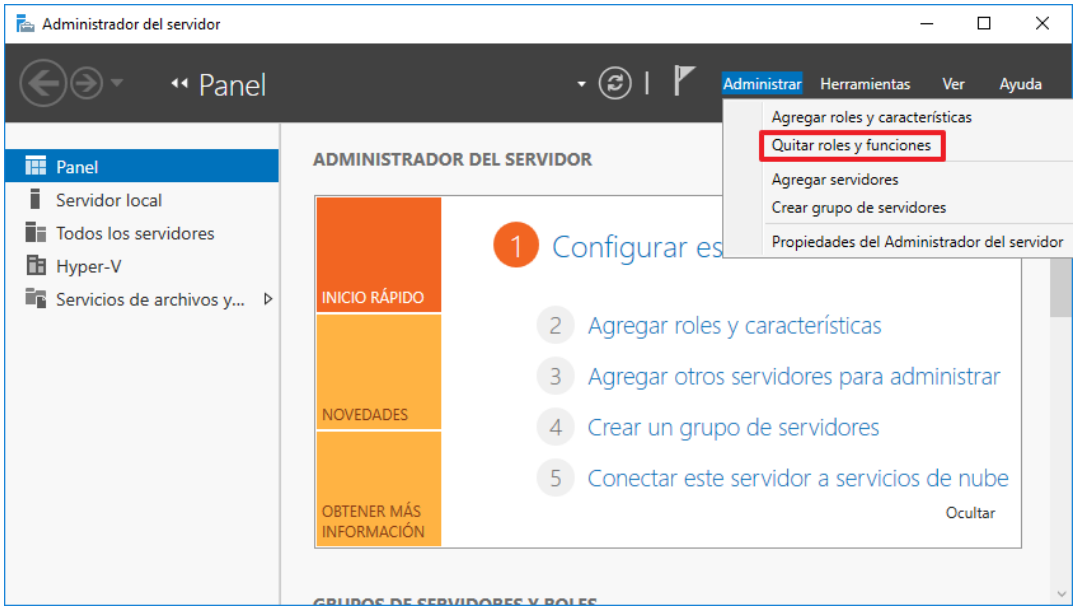
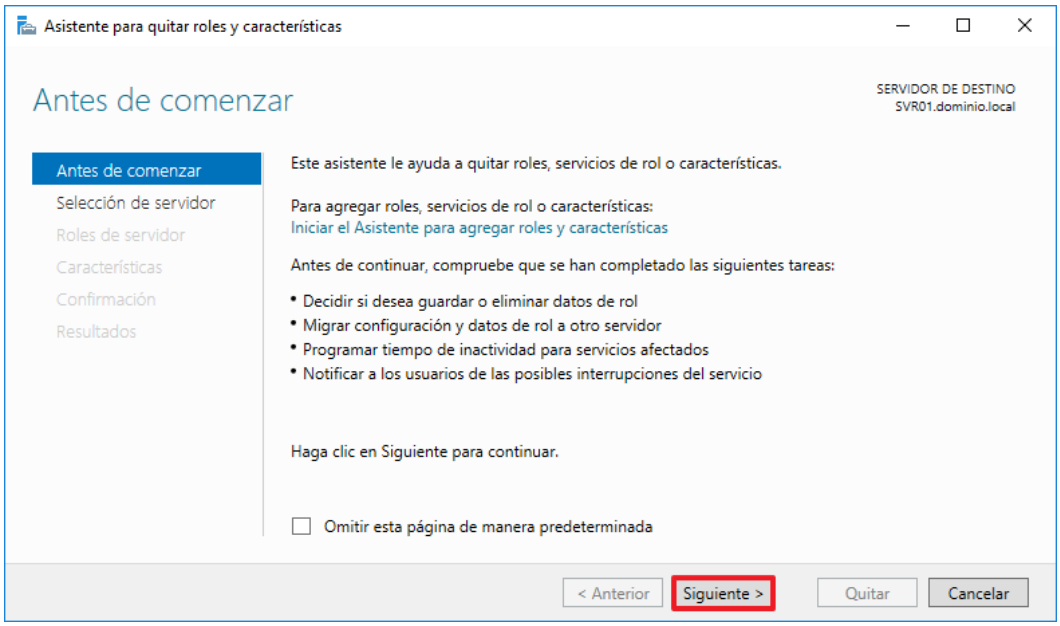
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

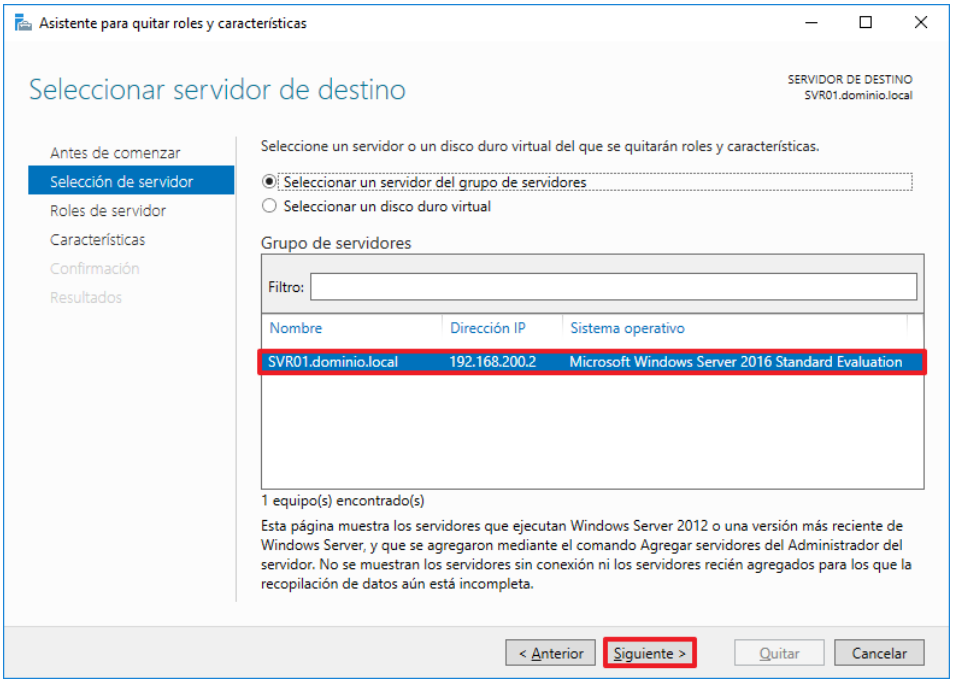
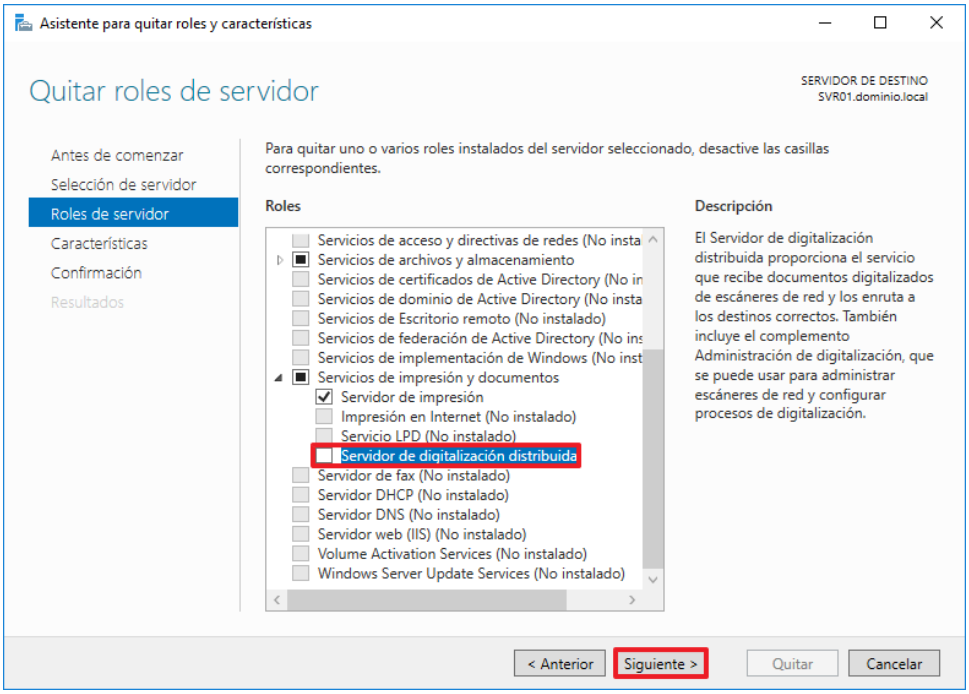
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

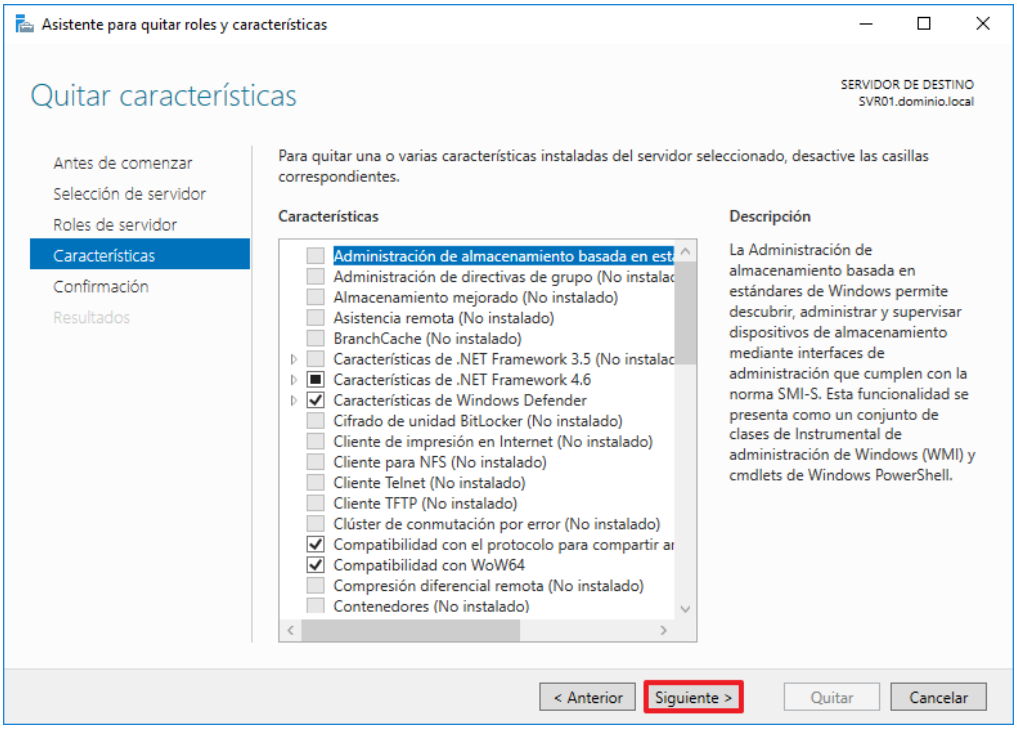
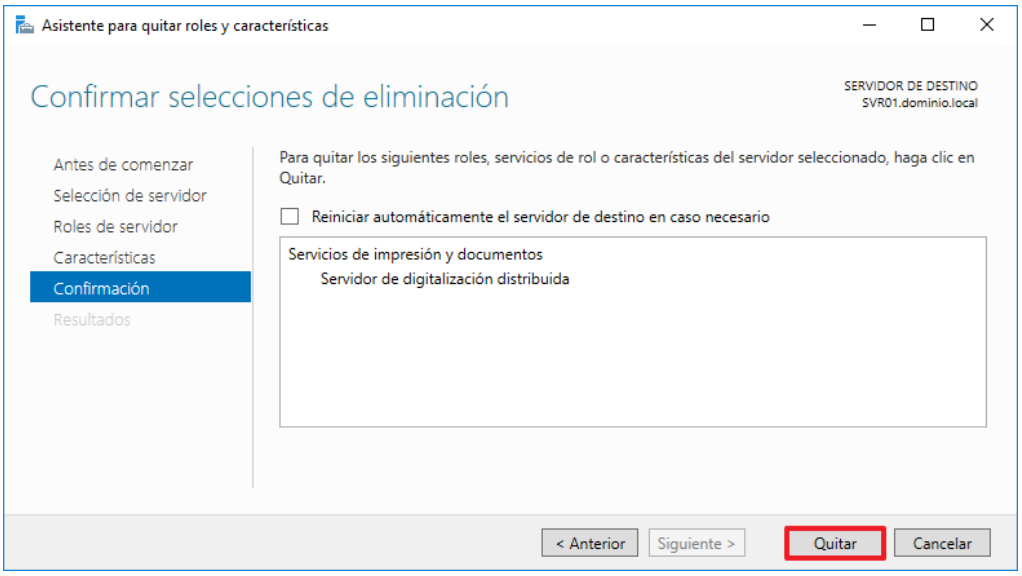
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

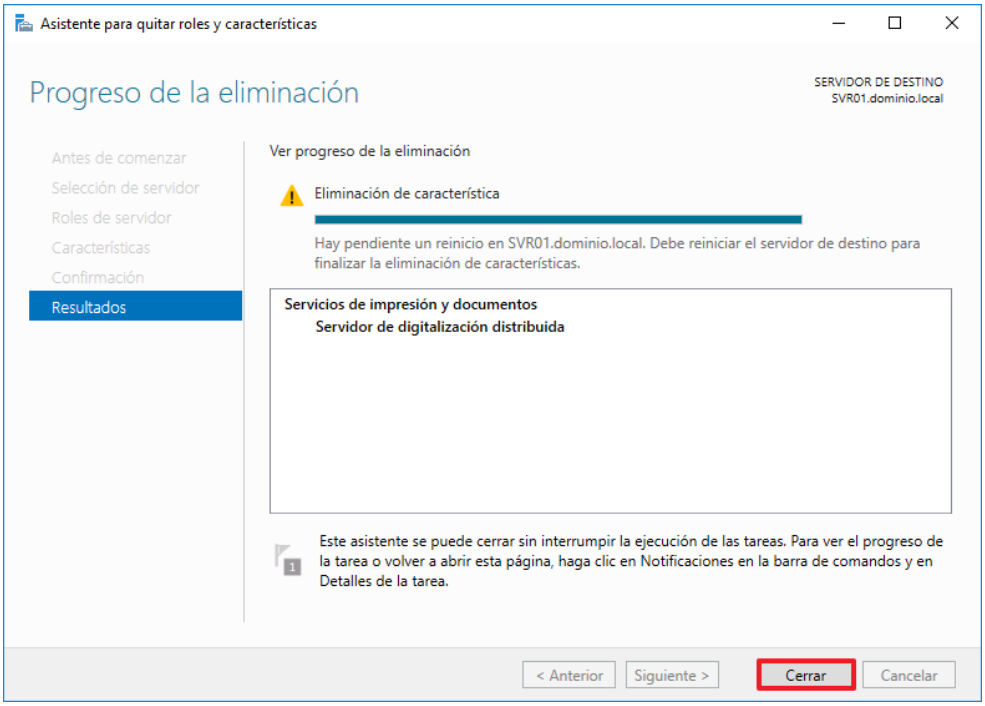
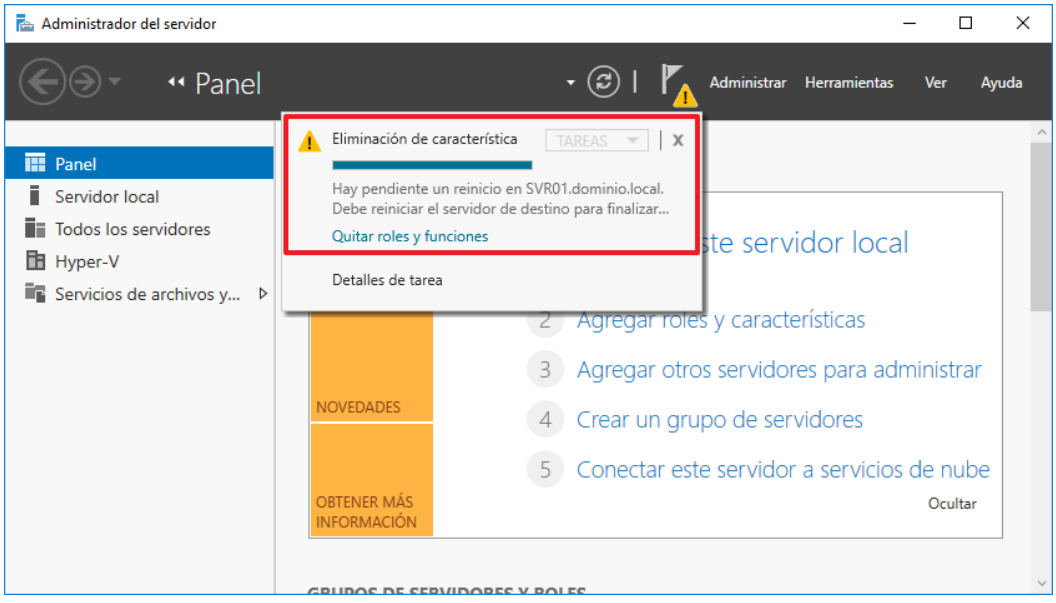
En el procedimiento que se describe a continuación, a modo de ejemplo, desinstala un rol que actualmente no está siendo utilizado.

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

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

Paso	Descripción
39.	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".
40.	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
41.	En la ventana de características pulse el botón "Siguiente >". En este ejemplo no se desinstala ninguna característica adicional. 
42.	En la ventana "Confirmación" pulse "Quitar" para iniciar el proceso. 

Paso	Descripción
43.	El proceso comenzará y una vez finalizado, y si todo ha ido bien bastará con pulsar sobre "Cerrar" para finalizar la desinstalación. 
44.	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. APLICACIÓN DE ESTÁNDARES INTERNACIONALES DE SEGURIDAD

Para que la instalación de SQL Server 2016 cumpla con los estándares internacionales de seguridad, se deben realizar una serie de configuraciones adicionales en el servidor, estas son:

a) Habilitar compatibilidad con dichos estándares de seguridad.

b) Instalar desencadenadores de inicio de sesión.

c) Establecer el proceso de rastreo.

Este procedimiento creará una serie de objetos en la base de datos (tablas, vistas, funciones, triggers y procedimientos almacenados) y un proceso de rastreo que incluye todos los eventos necesarios, junto a la garantía de que este proceso se inicia cada vez que se inicia el servidor. Los objetos creados son los siguientes:

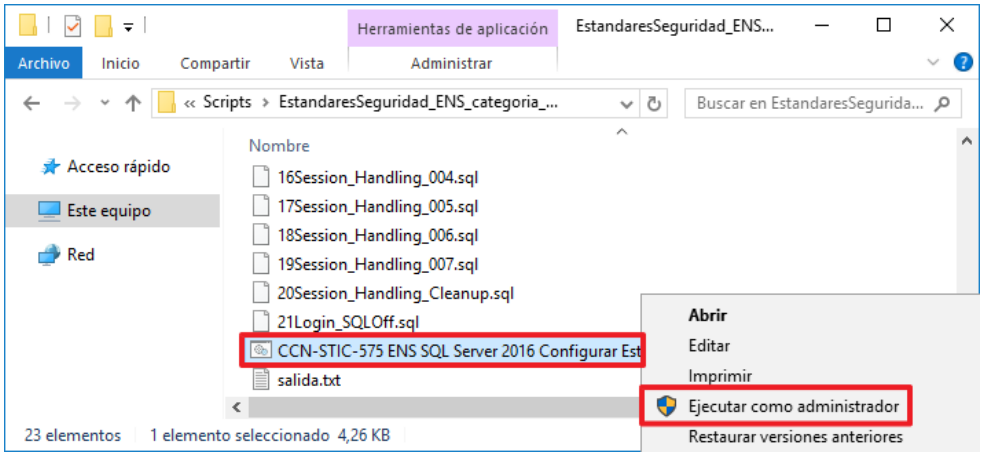
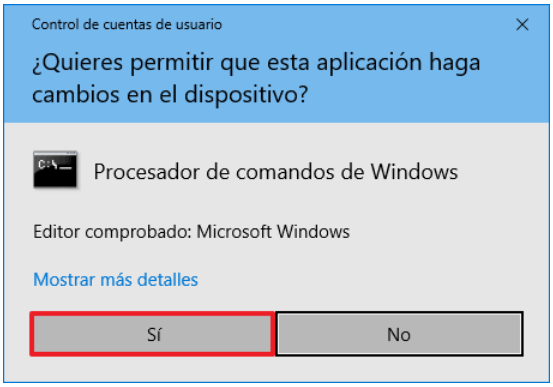
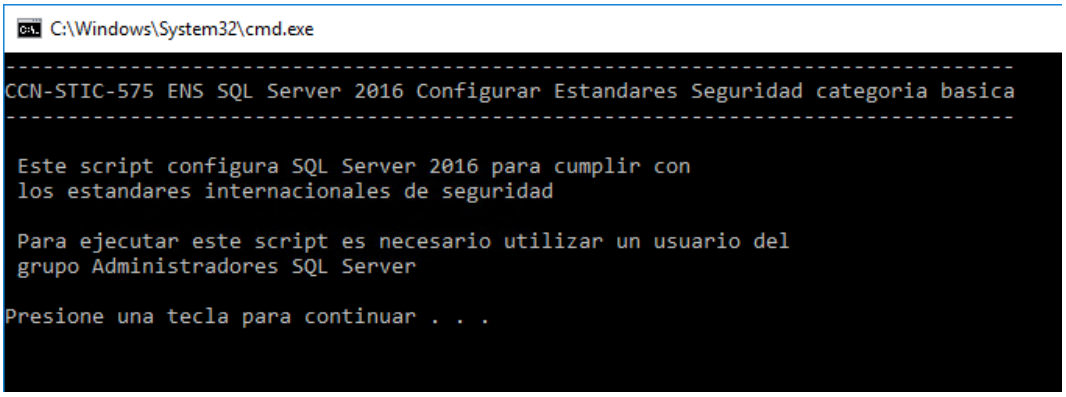
Objeto	Nombre	Descripción
Tabla	denied_logins_A54E382458CA11DB8373B622A1EF5492	Esta tabla contiene los intervalos semanales en la que los inicios de sesión no están autorizados a conectarse a SQL Server. Esta tabla no debe modificarse directamente.
Tabla	maximum_number_of_connections_per_login_A54E382458CA11DB8373B622A1EF5492	Esta tabla contiene el número máximo de conexiones por sesión. Esta tabla no debe modificarse directamente.
Vista	denied_logins	Esta vista vuelca el contenido de la tabla con los intervalos semanales en formato legible por los humanos.
Función	fn_is_original_login_denied_A54E382458CA11DB8373B622A1EF5492	Esta función comprueba si se permite el inicio de sesión original (la que creó la sesión) para iniciar sesión en este momento. El permiso EXECUTE para esta función se concede a todos los usuarios.
Trigger	trig_deny_access_A54E382458CA11DB8373B622A1EF5492	Este trigger se ejecuta en cada intento de inicio de sesión. Comprueba si el login tiene permitido iniciar sesión en ese momento (basado en la hora del día y el día de la semana) y si no se rechaza la conexión lanzando una excepción.
Trigger	trig_max_connections_A54E382458CA11DB8373B622A1EF5492	Este trigger se ejecuta en cada intento de inicio de sesión. Comprueba si el login tiene permitido iniciar sesión en ese momento (basado en el número máximo de sesiones concurrentes por usuario) y si no se rechaza la conexión lanzando una excepción.
Procedimiento almacenado	sp_deny_logon_internal_A54E382458CA11DB8373B622A1EF5492	Procedimiento interno que no debe ejecutarse directamente.
Procedimiento almacenado	sp_deny_logon	Este procedimiento almacenado permite al administrador negar el establecimiento de sesión a un cierto inicio de sesión basado en el día de la semana y la hora del día.

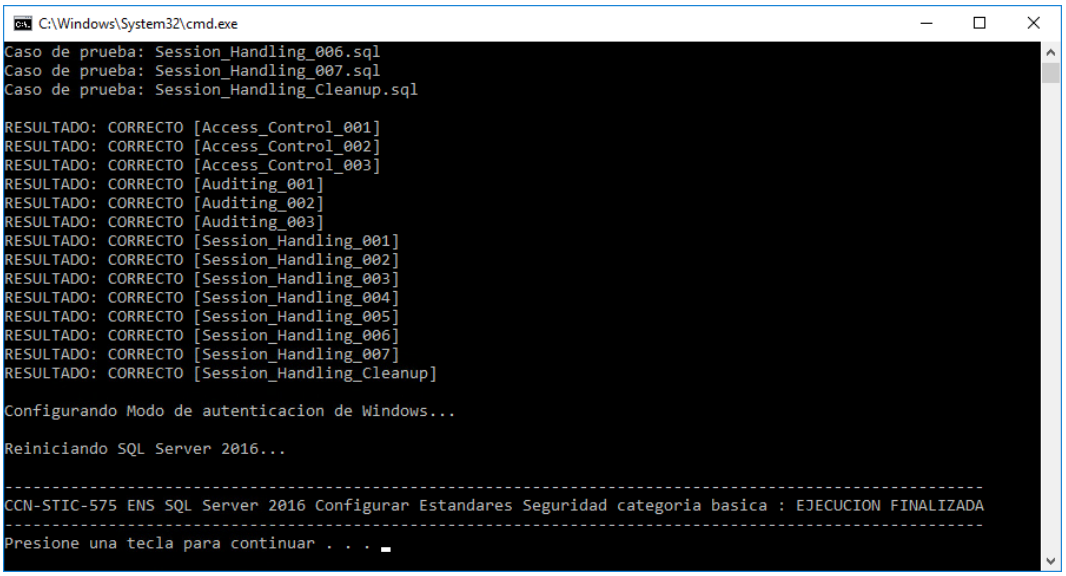
Objeto	Nombre	Descripción
Procedimiento almacenado	sp_revoke_logon_denies	Este procedimiento almacenado permite a un administrador revocar todas las denegaciones de un cierto inicio de sesión.
Procedimiento almacenado	sp_set_maximum_number_of_ connections_per_login	Este procedimiento almacenado permite a un administrador establecer el máximo número de conexiones concurrentes permitidas por inicio de sesión.
Procedimiento almacenado	sp_remove_maximum_number_of _connections_limit	Este procedimiento almacenado permite a un administrador eliminar la configuración del máximo número de conexiones concurrentes permitidas por inicio de sesión. Tras la ejecución de este procedimiento almacenado, SQL Server dejará de hacer cumplir cualquier limitación en el número de sesiones concurrentes por inicio de sesión.
Procedimiento almacenado	sp_trace_setcategory	Este procedimiento almacenado permite a un administrador habilitar o deshabilitar una columna de datos específica para todos los eventos en una categoría de traza determinada.
Procedimiento almacenado	sp_trace_setcategory_all	Este procedimiento almacenado permite a un administrador habilitar o deshabilitar todas las columnas de datos válidas para todos los eventos en una categoría de traza determinada.

Como resultado del proceso de rastreo, se generarán una serie de ficheros de traza en la carpeta Log de la carpeta raíz de la instancia SQL Server instalada, donde se registrarán todos los eventos. Además, durante la ejecución de esta fase se activa la auditoría de inicios de sesión correctos y erróneos.

A continuación, se muestran los pasos necesarios para llevar a cabo esta configuración.

Paso	Descripción
45.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
46.	Localice la carpeta "C:\Scripts\EstandaresSeguridad_ENS_categoria_basica" que previamente se ha copiado al equipo. **Nota:** En caso de no disponer de la carpeta "C:\Scripts" deberán copiar los archivos necesarios en la ruta "C:\Scripts" para continuar con la ejecución del paso a paso.

Paso	Descripción
47.	Ejecute el script "CCN-STIC-575 ENS SQL Server 2016 Configurar Estandares Seguridad categoria basica.bat" con privilegios de administración. Para ello, pulse con el botón derecho "Ejecutar como administrador". 
48.	El "Control de cuentas de usuarios" le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador de dominio y pulse "Sí". 
49.	A continuación, pulse cualquier tecla para aplicar los estándares internacionales de seguridad. 

Paso	Descripción
50.	Espere a que finalice el proceso. Puede tardar varios minutos en completarse. Una vez finalizada la configuración, presione una tecla para cerrar la ventana.  **Nota:** Omita cualquier advertencia de error que se encuentre fuera del rango de valores "Resultado".
51.	Compruebe que el resultado de todas las pruebas es "CORRECTO". **Nota:** Durante este proceso se activa el modo de autenticación de Windows y SQL para poder llevar a cabo parte de las pruebas. Al finalizar el proceso se vuelve a configurar el Modo de autenticación de Windows.
52.	Pulse una tecla para finalizar la ejecución de la configuración y cerrar la ventana.
53.	Para que el sistema termine de aplicar los cambios deberá reiniciar el servidor donde se están aplicando las configuraciones de seguridad.

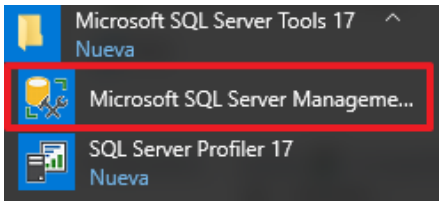
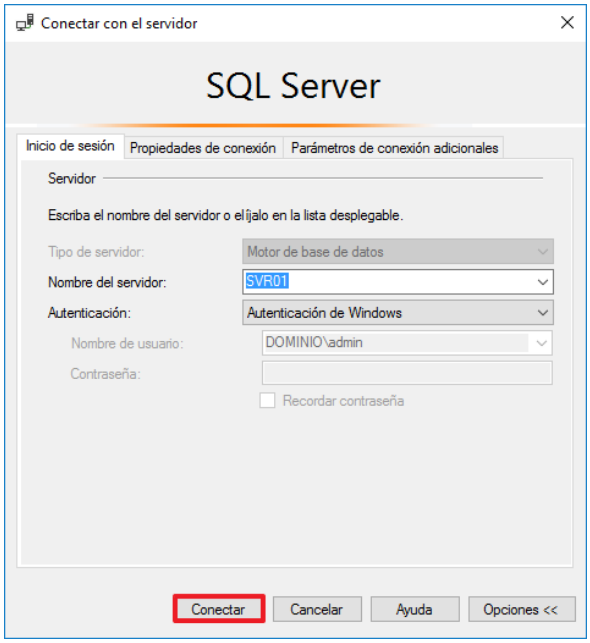
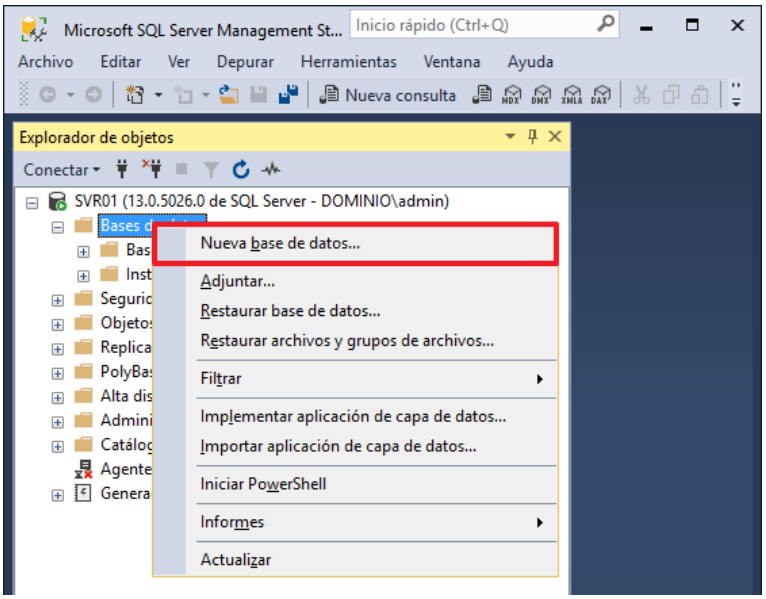
2.3. GESTIÓN DE BASES DE DATOS

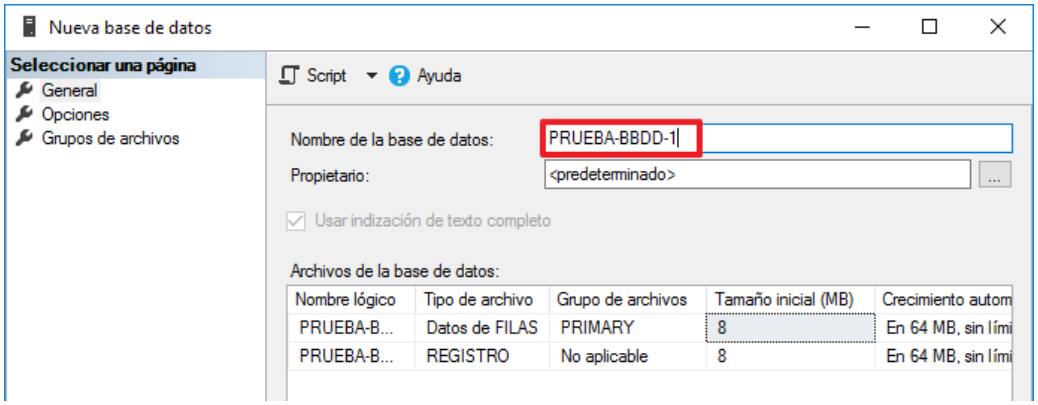
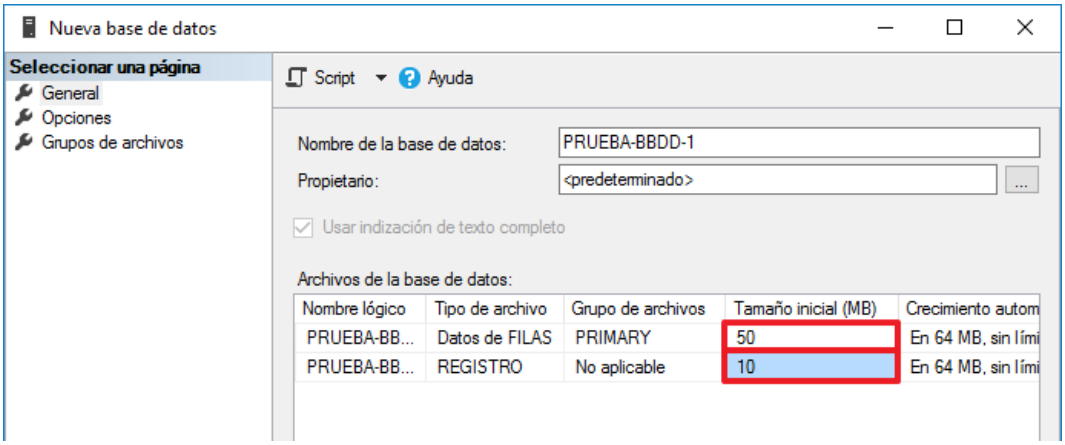
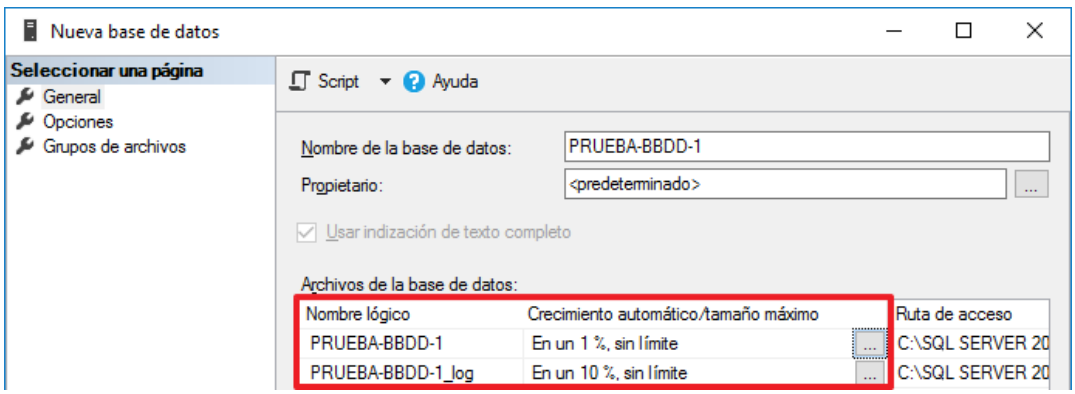
Las bases de datos son el componente sobre el que se apoya SQL Server 2016 para almacenar toda la información que se genera. Este apartado define un ejemplo de cómo gestionar dichas bases de datos.

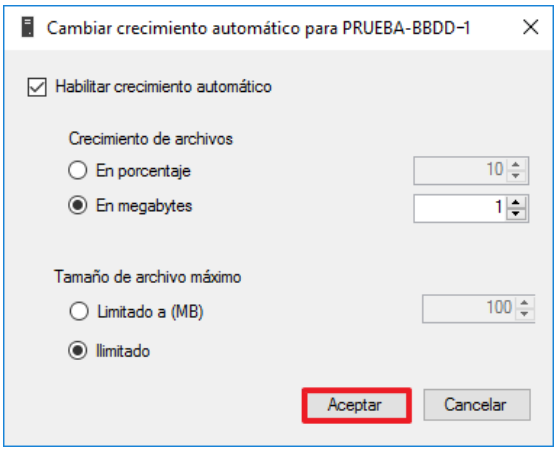
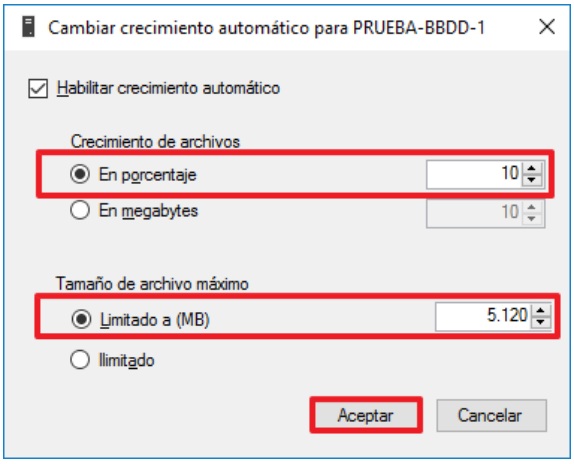
2.3.1. CREACIÓN DE BASES DE DATOS

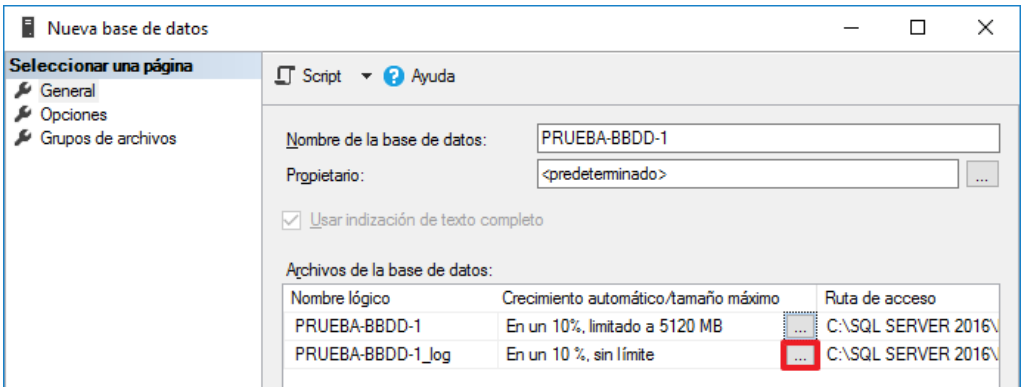
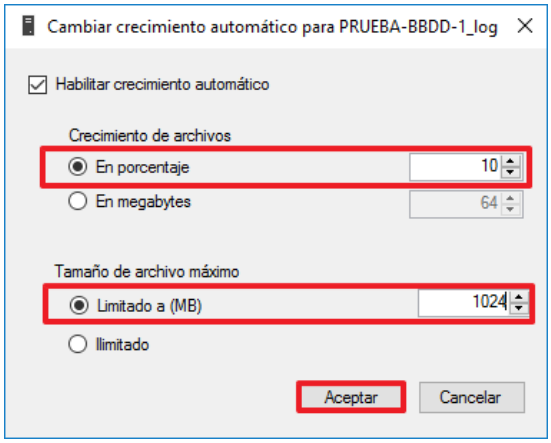
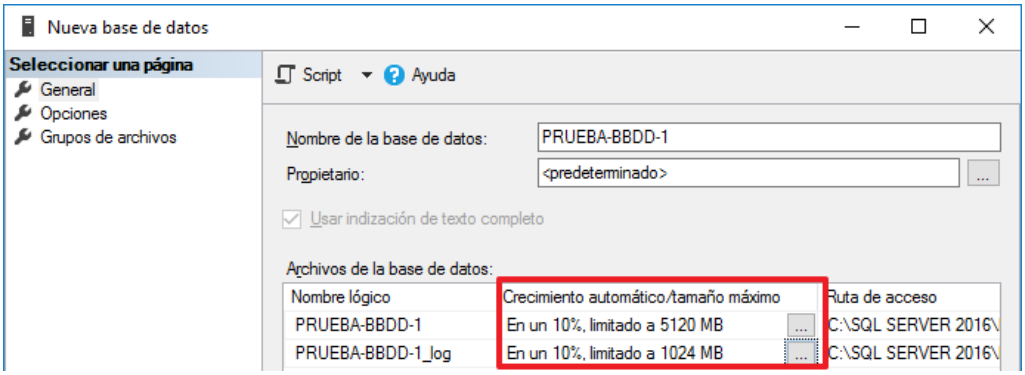
En esta sección se definen los pasos para crear una nueva base de datos en el servidor SQL.

Paso	Descripción
54.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.

Paso	Descripción
55.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
56.	En la ventana de "Conectar con el servidor", es necesario asegurarse que el nombre del servidor es el correcto y pulse "Conectar". 
57.	Despliegue el nodo "Bases de datos" y con el botón derecho, seleccione la opción del menú contextual "Nueva base de datos". 

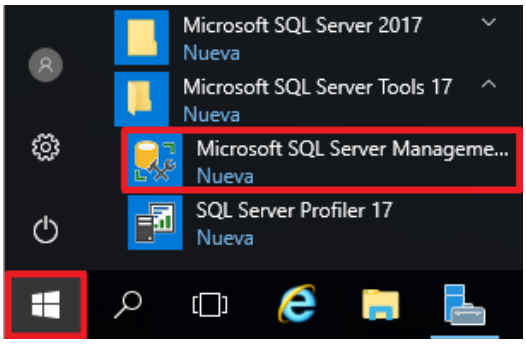
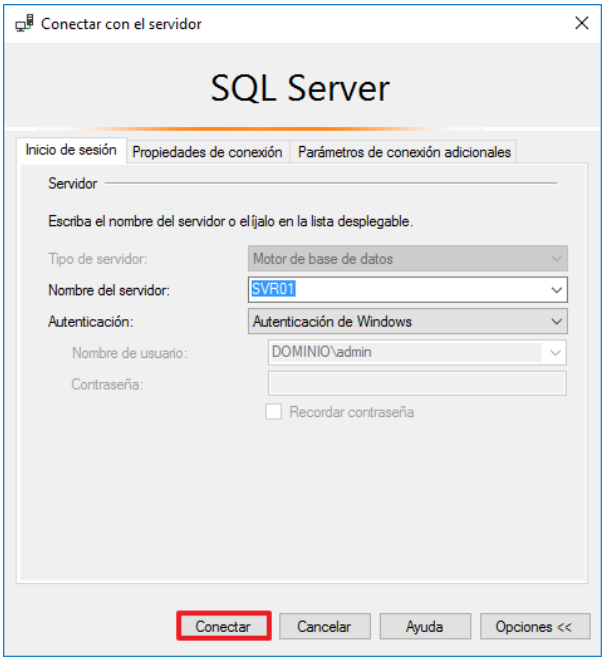
Paso	Descripción
58.	Escriba el nombre de la base de datos que se desea crear.  **Nota:** En este ejemplo se utiliza el nombre "PRUEBA-BBDD-1".
59.	En la zona de archivos de la base de datos, puede especificar el tamaño inicial de la base de datos y el grado de crecimiento automático que se desea aplicar. Por ejemplo, si desea crear una base de datos con 50 MB de tamaño inicial y un fichero de registro de transacciones (log) con 10 MB, entonces establezca los valores 50 y 10 respectivamente. 
60.	En la columna de crecimiento automático, se establece el grado de crecimiento que se desea implementar para ambos ficheros una vez que se haya alcanzado el tamaño inicial establecido. 

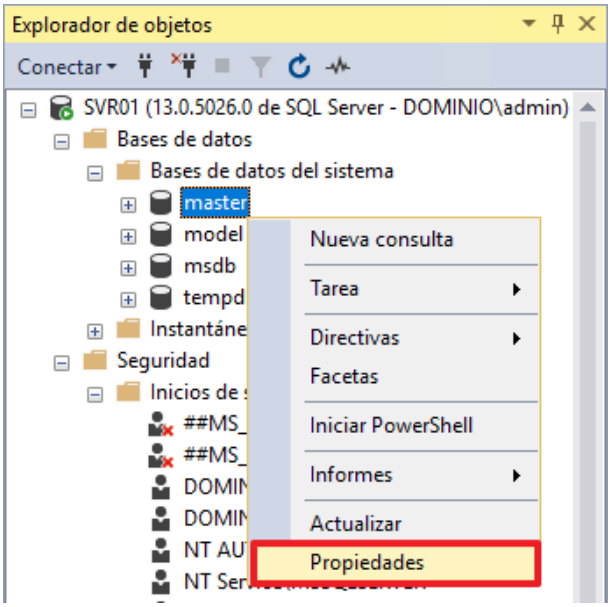
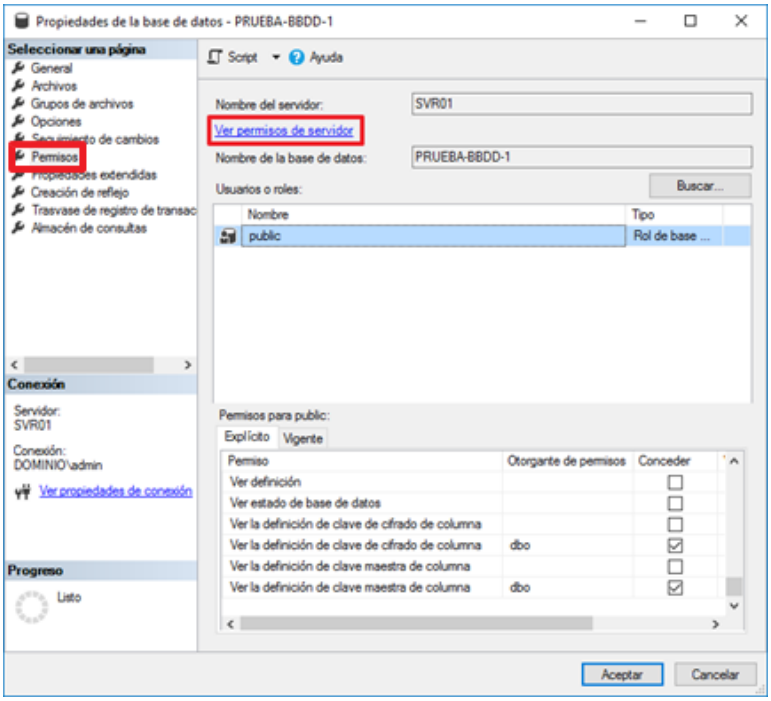
Paso	Descripción
61.	Pulse sobre el primero de los botones "…" para establecer el grado de crecimiento de la base de datos. Pulse "Aceptar" para guardar los cambios.  **Nota:** Puede establecerse el crecimiento en un porcentaje relativo al tamaño de la base de datos o en un valor estático en megabytes (MB). También puede limitarse el crecimiento a un tamaño máximo, para evitar que se pueda consumir todo el espacio del disco físico.
62.	En este ejemplo se va a configurar el crecimiento automático en un porcentaje de 10%, con un límite máximo de 5 GB para la base de datos y 1 GB para el fichero de registro de transacciones.
63.	Seleccione la opción "En porcentaje" y escriba 10. A continuación seleccione "Limitar el crecimiento de los archivos (MB)" y escriba 5120. Pulse sobre el botón "Aceptar". 

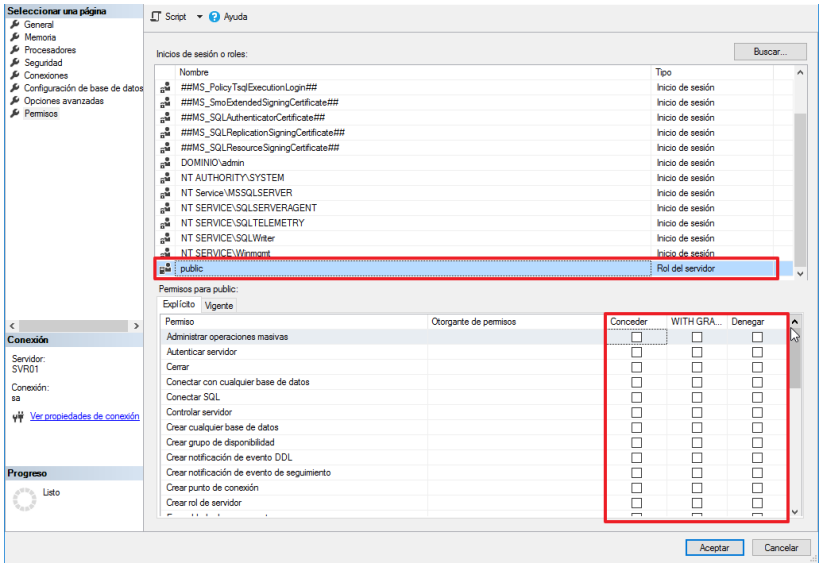
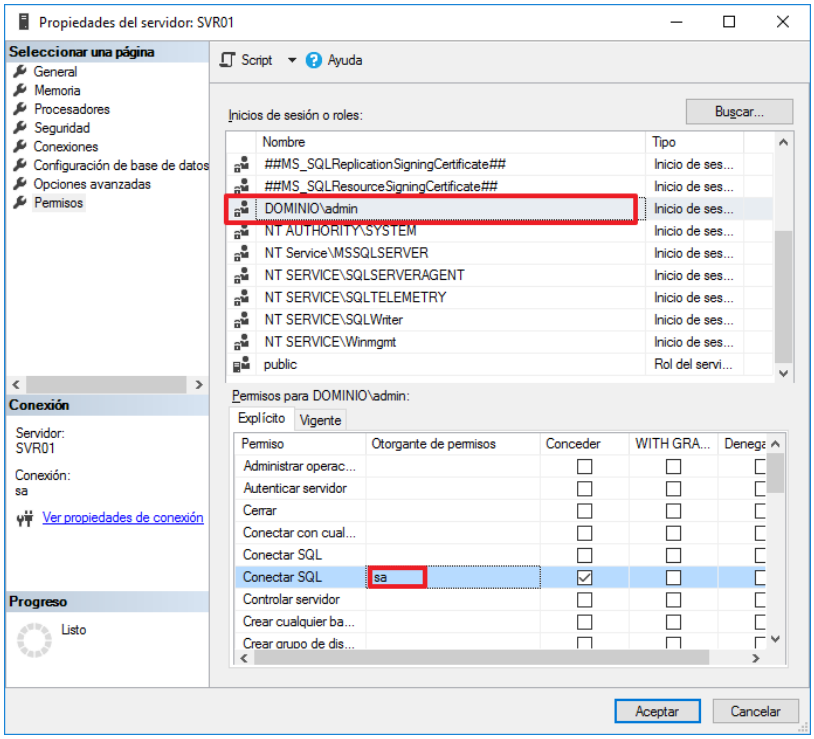
Paso	Descripción
64.	Pulse sobre el segundo de los botones "…" para establecer el grado de crecimiento del fichero de registro de transacciones de la base de datos. 
65.	Debe seleccionarse la opción "En porcentaje" y escriba 10. A continuación seleccione la opción "Limitado a (MB)" y escriba 1024. Pulse sobre el botón "Aceptar". 
66.	Compruebe que los valores introducidos son correctos. 

2.3.2. MODIFICACIÓN DE BASES DE DATOS

En esta sección se definen los pasos para modificar parámetros de seguridad de una base de datos en el servidor SQL.

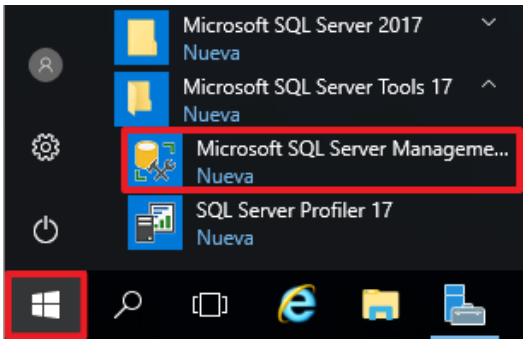
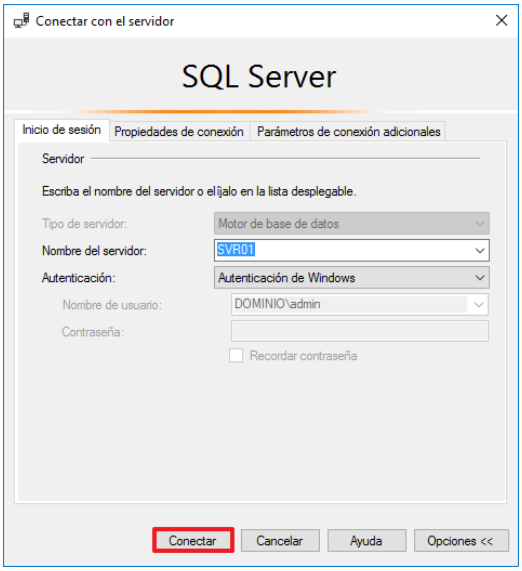
Paso	Descripción
67.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
68.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
69.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar". 

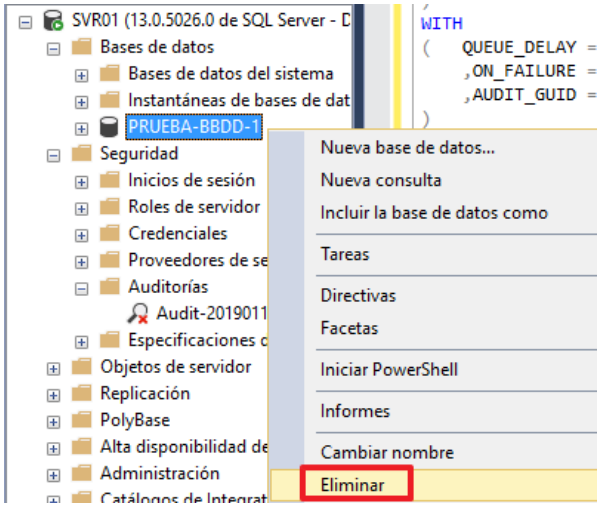
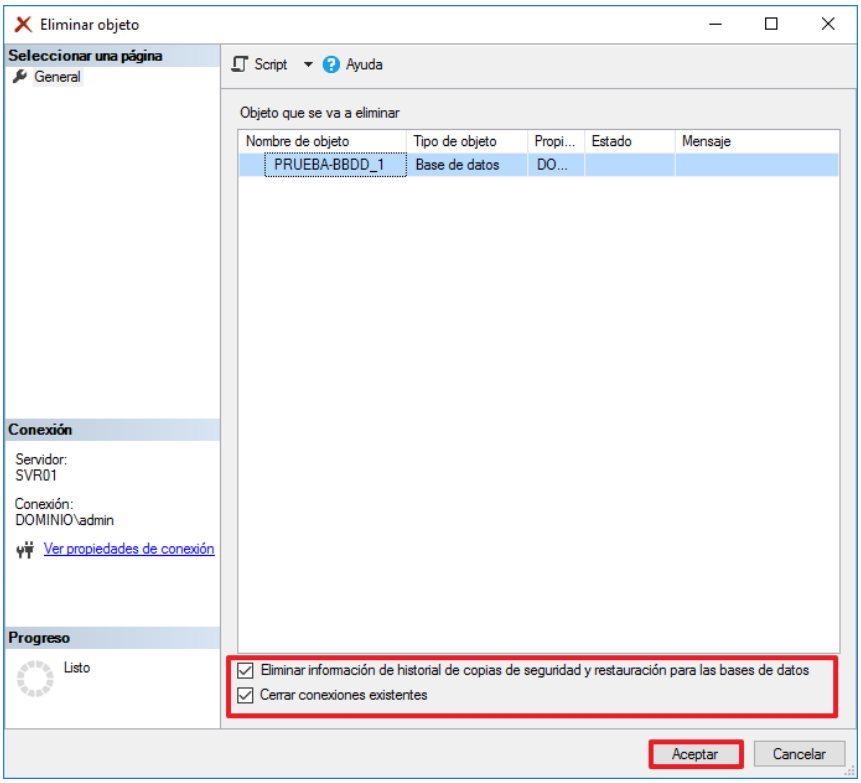
Paso	Descripción
70.	En la consola "SQL Server Management Studio", seleccione el nodo "Bases de datos" y diríjase a la base de datos que quiera modificar dentro de "Bases de datos del sistema".  **Nota:** En este ejemplo, se modificará la base de datos "master".
71.	Seleccione la pestaña "Permisos" en el panel izquierdo y finalmente pulse la opción "Ver permisos del servidor". 

Paso	Descripción
72.	En esta pantalla puede cambiar los permisos de cada inicio de sesión y/o rol del servidor. marcando los distintos inicios de sesión en el panel superior se muestran los permisos de éste. 
73.	Es necesario asegurarse que después de haber dado de alta todos los inicios de sesión necesarios de su organización tan sólo un inicio de sesión o rol puede cambiar los permisos del resto de usuarios tal y como se ve en la siguiente pantalla.  **Nota:** Para más información sobre los servicios de servidores asociados a las cuentas de SQL Server puede consultar la página https://docs.microsoft.com/es-es/sql/database-engine/configure-windows/configure-windows-service-accounts-and-permissions?view=sql-server-2016.

2.3.3. ELIMINACIÓN DE BASES DE DATOS

En esta sección se definen los pasos para eliminar una base de datos en el servidor SQL.

Paso	Descripción
74.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
75.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
76.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar". 

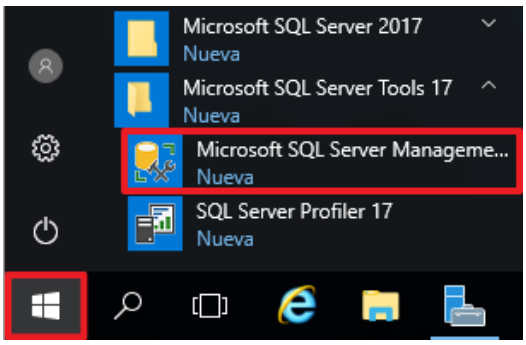
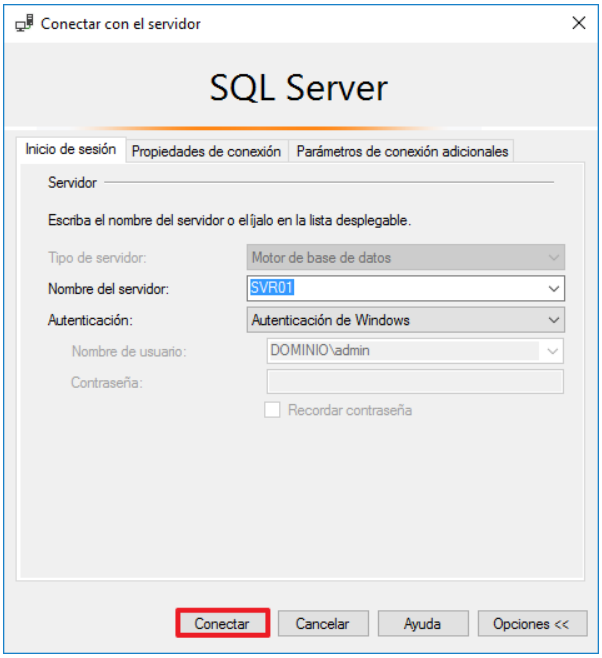
Paso	Descripción
77.	Sitúese en el nodo del árbol "Bases de datos" y seleccione la base de datos que quiera eliminar. Haga clic derecho sobre ella y pulse "Eliminar".  **Nota:** En este ejemplo se procede a eliminar la base de datos llamada "PRUEBA-BBDD-1".
78.	En la siguiente pantalla, marque las opciones "Eliminar información de historial de copias de seguridad y restauración para las bases de datos" y "Cerrar conexiones existentes", finalmente pulse "Aceptar" para eliminar la base de datos. 

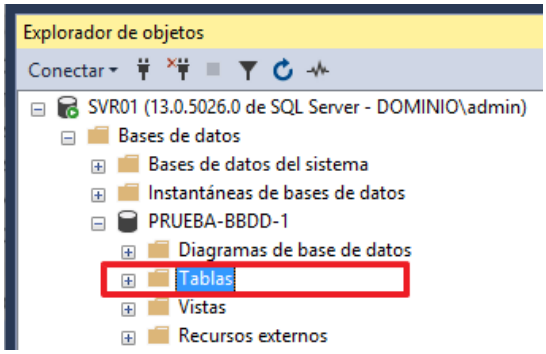
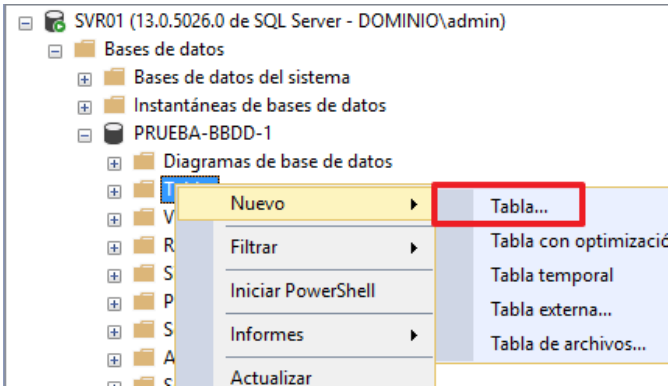
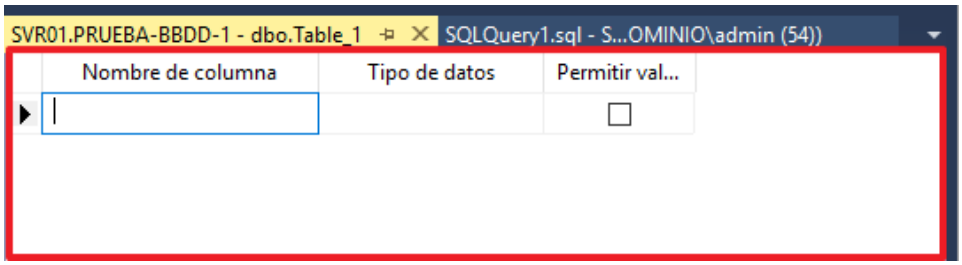
2.4. GESTIÓN DE TABLAS

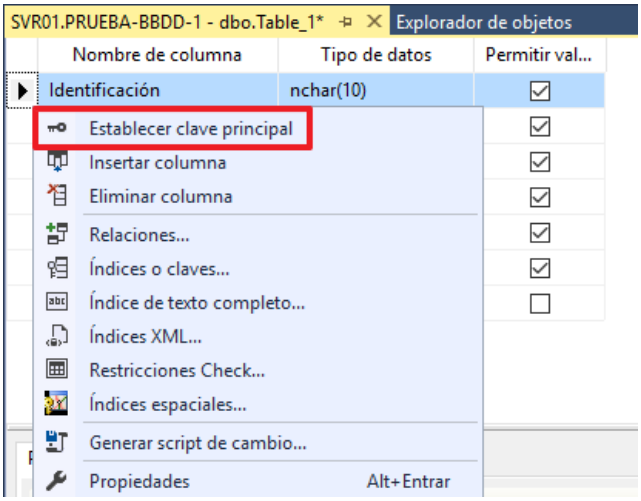
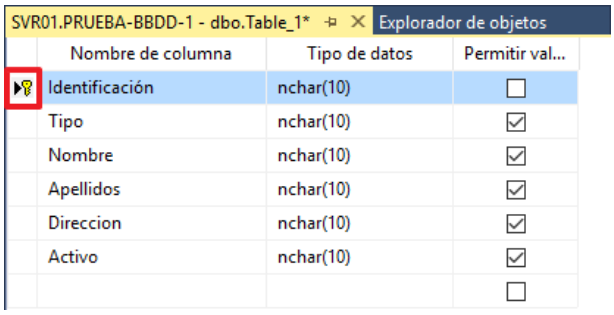
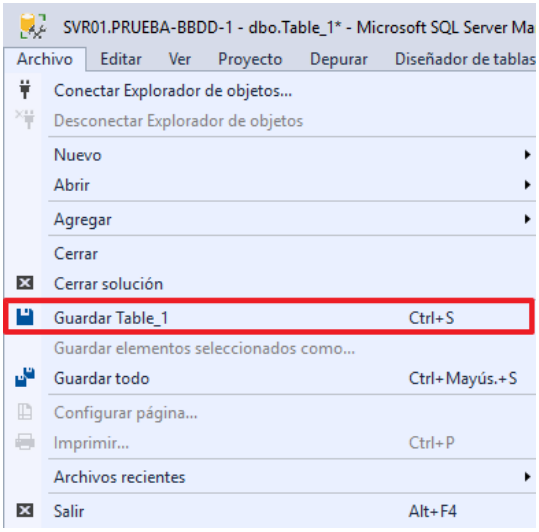
La gestión de tablas dentro de SQL Server 2016 constituye una importante tarea de administración debido a que permite establecer o modificar configuraciones que afectan a la funcionalidad del servicio de base de datos.

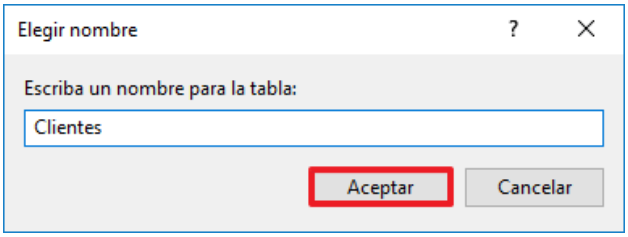
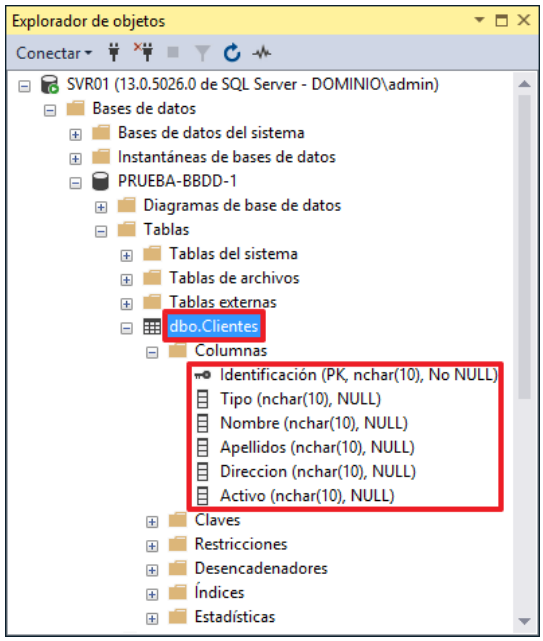
2.4.1. CREACIÓN DE TABLAS

En este apartado se definen los pasos para crear una nueva base de datos en el servidor SQL.

Paso	Descripción
79.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
80.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".** 
81.	En la ventana de "Conectar con el servidor", asegúrese de que el nombre del servidor es el correcto y pulse "Conectar". 

Paso	Descripción
82.	En la consola "SQL Server Management Studio", sitúese en la base de datos donde desee crear una nueva tabla y diríjase a la carpeta "Tablas". la carpeta "Tablas" de la base de datos "PRUEBA-BBDD-1" creada anteriormente, tal y como se observa en la imagen.  **NOTA:** En este ejemplo, se procede a crear una tabla dentro de la base de datos "PRUEBA-BBDD-1".
83.	Con el botón derecho sobre "Tablas", seleccione la opción del menú contextual **"Nuevo → Tabla…".** 
84.	En el área "Nombre de columna", establezca un nombre a cada una de las columnas que va a tener la nueva tabla, así como el tipo de dato correspondiente.  **Nota:** Se recomienda no incluir caracteres especiales en los nombres de las columnas, tales como tildes, signos de exclamación, interrogación o cedillas.

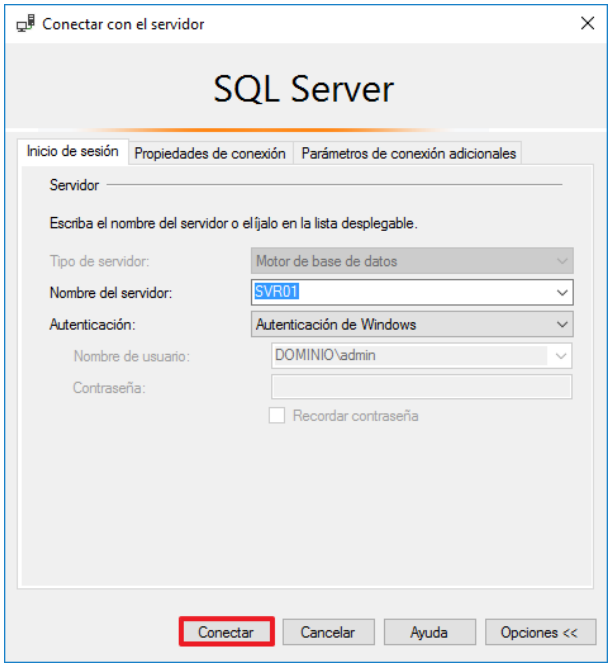
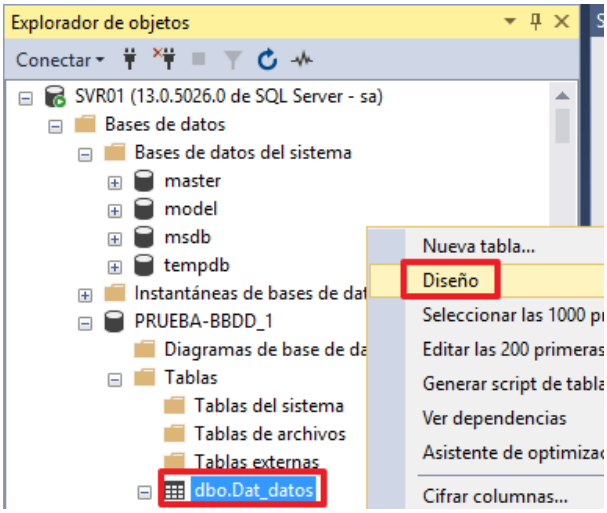
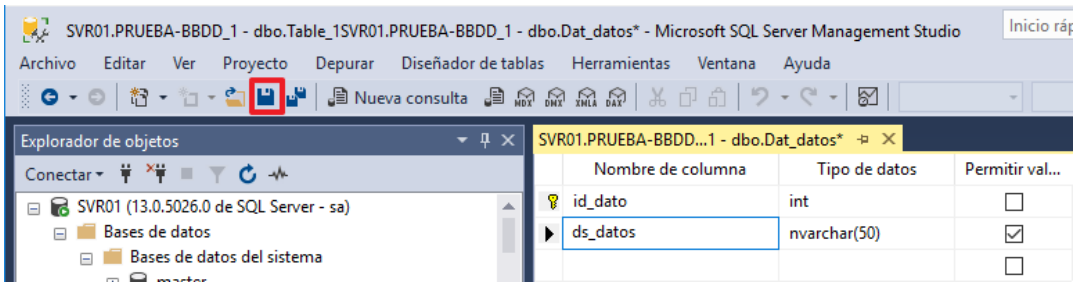
Paso	Descripción
85.	Cuando haya finalizado de introducir las diferentes columnas, será necesario establecer una clave principal dentro de la nueva tabla. Para ello, seleccione aquella columna que desea establecer como llave primaria y pulsando con el botón derecho sobre ella, seleccione la opción del menú contextual "Establecer clave primaria".  **Nota:** En este ejemplo, se utiliza la columna "Identificación".
86.	Asegúrese que aparece una llave sobre la columna que ha establecido como clave primaria como se muestra en la siguiente imagen. 
87.	Para guardar los cambios realizados, pulse sobre la opción del menú contextual **"Archivo → Guardar Table_1".** 

Paso	Descripción
88.	Establezca un nombre para la nueva tabla acorde a las necesidades de su organización y pulse sobre el botón "Aceptar".  **Nota:** En este ejemplo, se utiliza el nombre "Clientes".
89.	Ahora, en el Explorador de objetos, acceda a la nueva tabla para obervar las columnas creadas en pasos anteriores. 

2.4.2. MODIFICACIÓN DE TABLAS

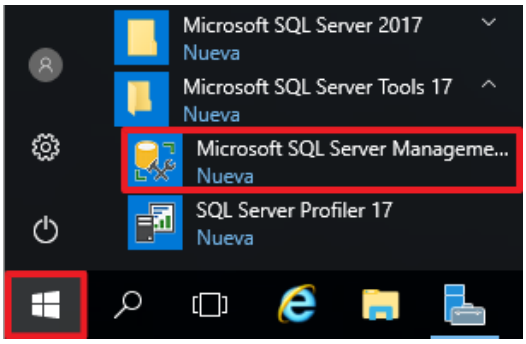
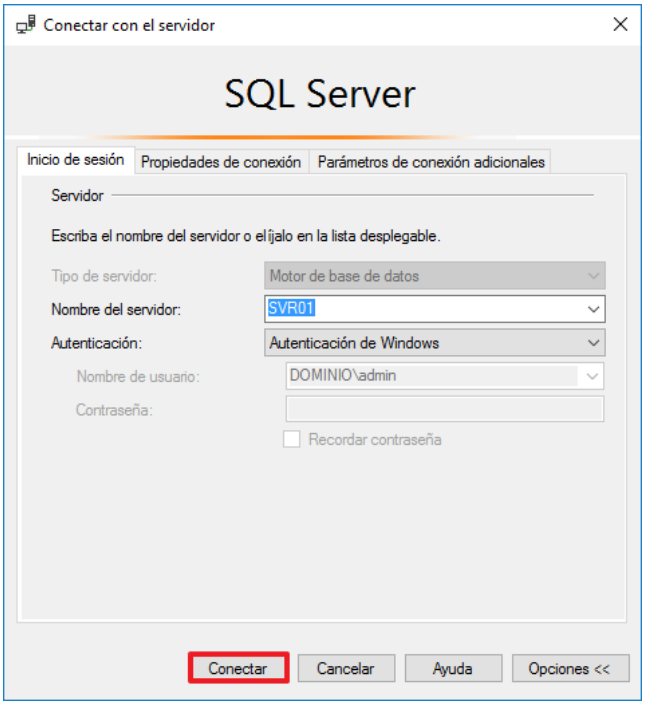
En este apartado se define como modificar una tabla desde SQL Server Management Studio.

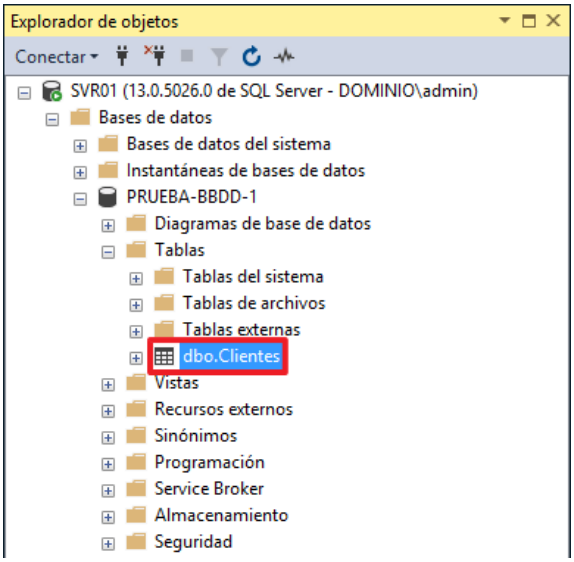
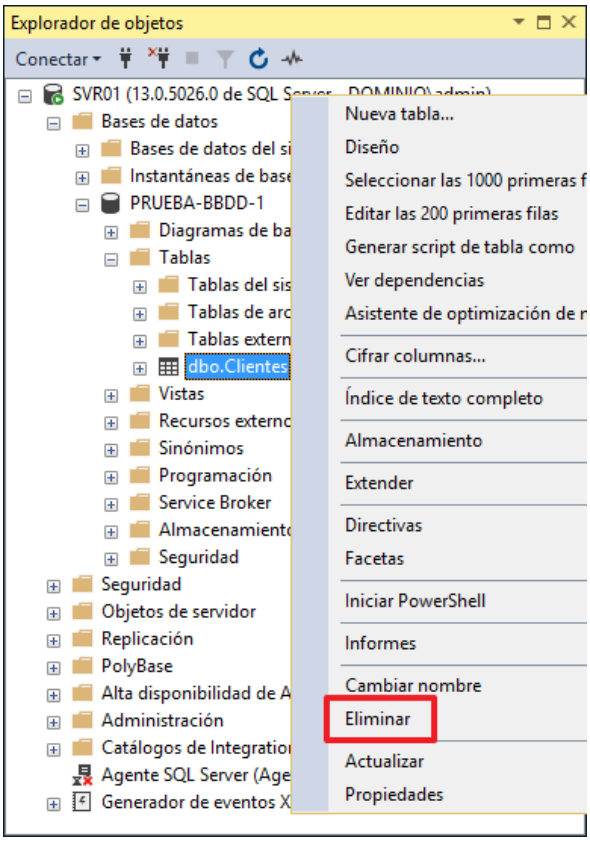
Paso	Descripción
90.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
91.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**.

Paso	Descripción
92.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar". 
93.	En la consola "SQL Server Management Studio" localice la tabla que desea modificar, y pulsando con el botón derecho sobre ella, seleccione la opción "Diseño". 
94.	Ahora, podrá realizar los cambios que considere oportunos para su organización. Para guardar los cambios, pulse el botón "guardar". 

2.4.3. ELIMINACIÓN DE TABLAS

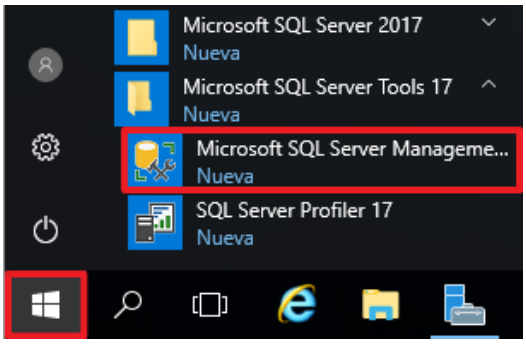
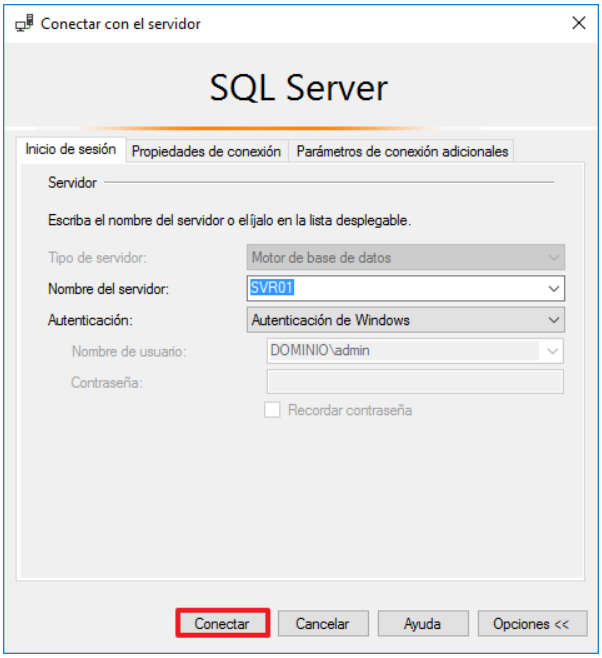
En este apartado se define como eliminar una tabla desde SQL Server Management Studio.

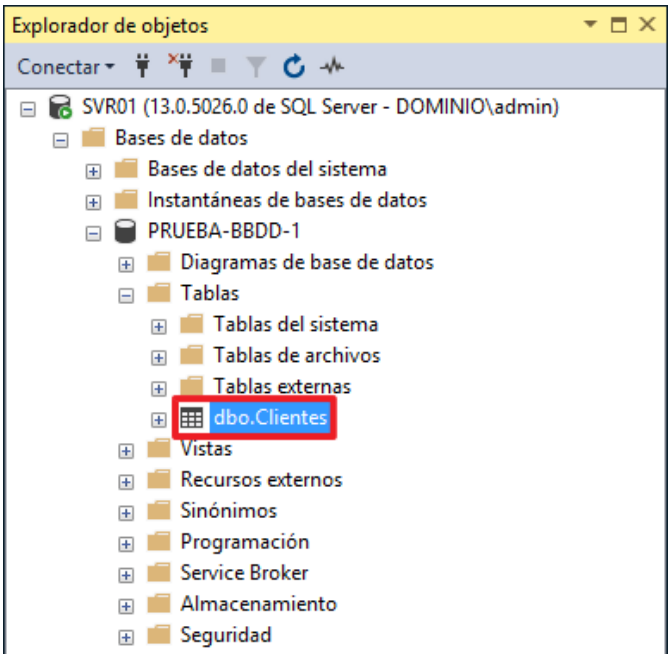
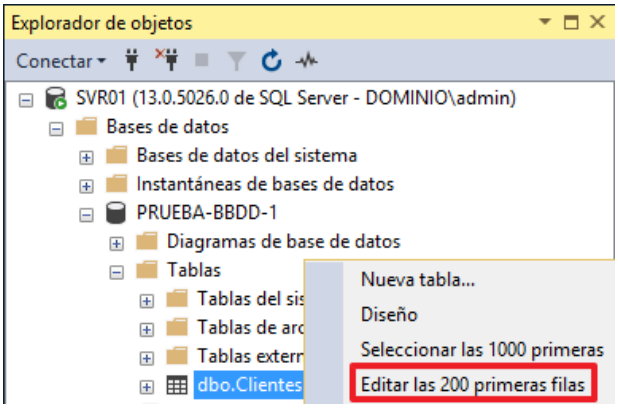
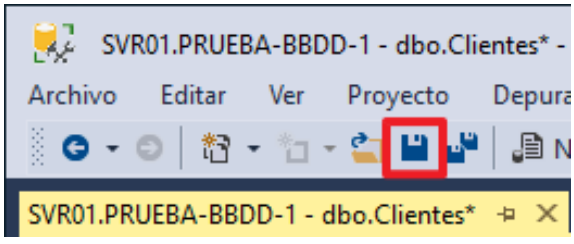
Paso	Descripción
95.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
96.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".** 
97.	En la ventana de "Conectar con el servidor", asegúrese de que el nombre del servidor es el correcto y pulse "Conectar". 

Paso	Descripción
98.	Dentro del Explorador de objetos, expanda el árbol "Bases de datos" hasta llegar a la tabla que desea eliminar.  **Nota:** En este ejemplo, se utiliza la tabla "dbo.Clientes"
99.	Una vez seleccionada la tabla, haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Eliminar". 

2.4.4. INSERCIÓN DE DATOS

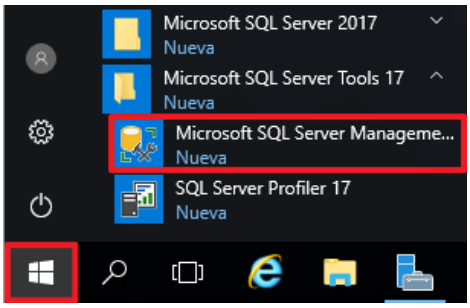
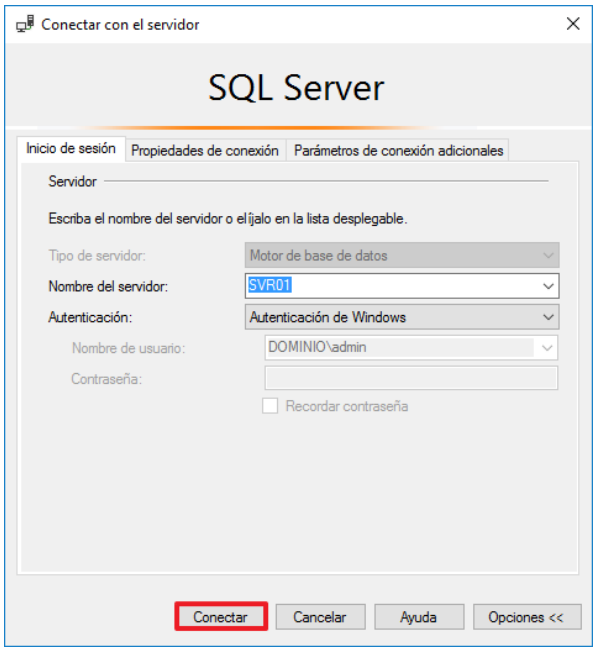
En este apartado se define como insertar datos desde SQL Server Management Studio.

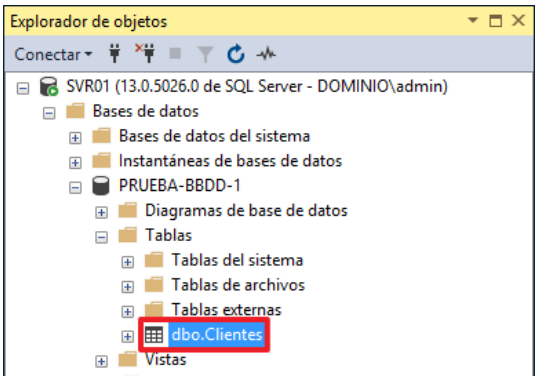
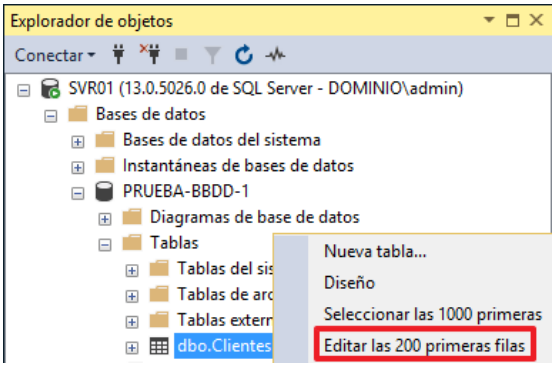
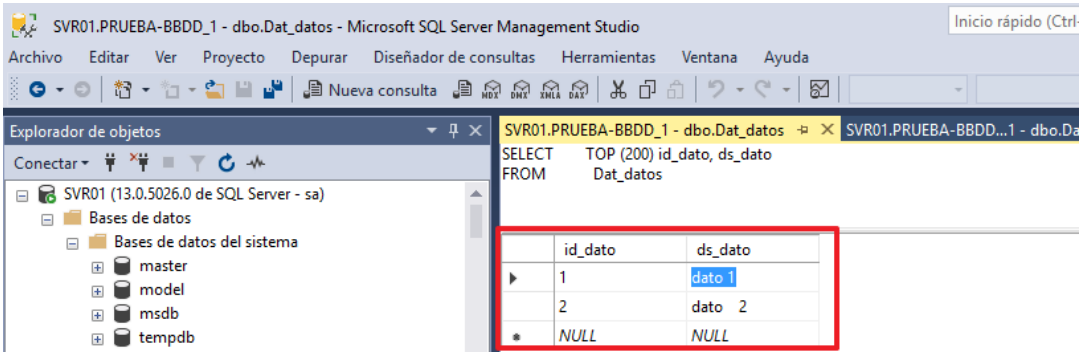
Paso	Descripción
100.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
101.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
102.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar". 

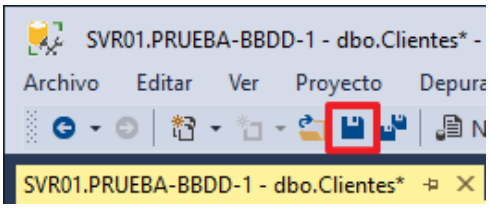
Paso	Descripción
103.	Dentro del Explorador de objetos, expanda el árbol "Bases de datos" hasta llegar a la tabla que desea insertar datos.  **Nota:** En este ejemplo, se utiliza la tabla "dbo.Clientes".
104.	Una vez seleccionada la tabla, haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Editar las 200 primeras filas" para insertar los datos en la tabla seleccionada. 
105.	Una vez finalizada la inserción de datos, pulse el botón "Guardar" para salvaguardar los datos introducidos. 

2.4.5. MODIFICACIÓN DE DATOS

En este apartado se define como modificar datos desde SQL Server Management Studio.

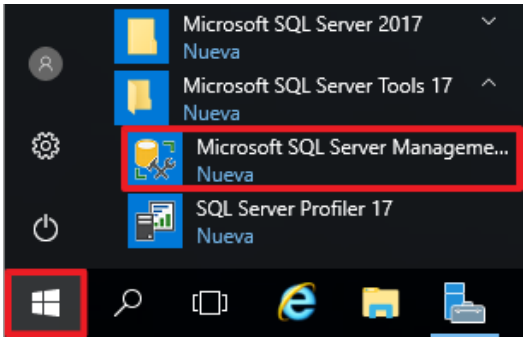
Paso	Descripción
106.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
107.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
108.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar". 

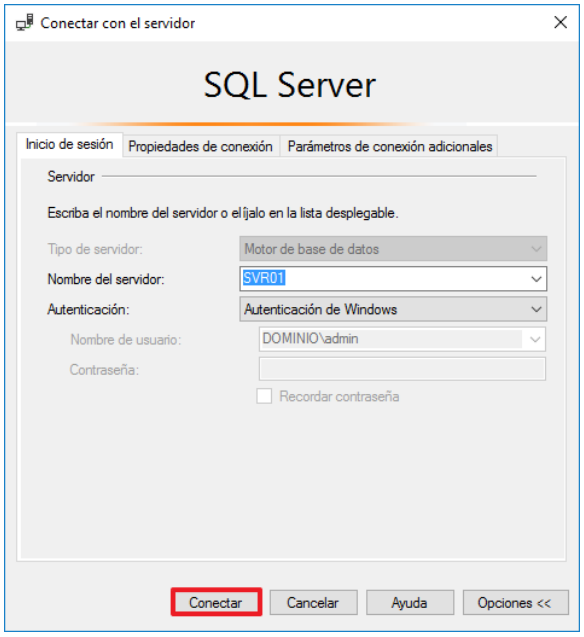
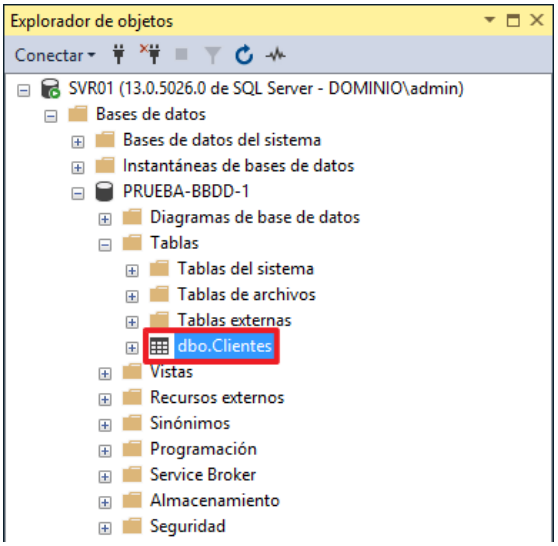
Paso	Descripción
109.	Dentro del Explorador de objetos, expanda el árbol "Bases de datos" hasta llegar a la tabla que desea insertar datos.  **Nota:** En este ejemplo, se utiliza la tabla "dbo.Clientes".
110.	Una vez seleccionada la tabla, haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Editar las 200 primeras filas". 
111.	En la siguiente ventana, puede insertar y modificar los datos acorde a las necesidades de su organización. 

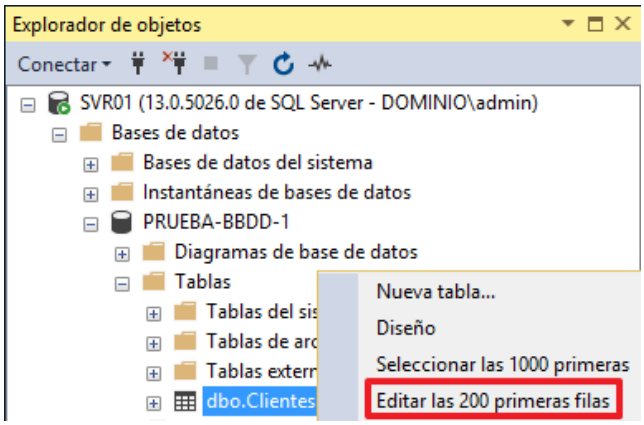
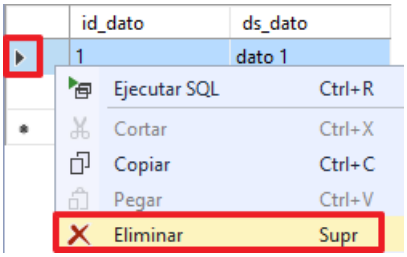
Paso	Descripción
112.	Una vez finalizada la modificación de datos, pulse el botón "Guardar" para salvaguardar los datos modificados. 

2.4.6. ELIMINACIÓN DE DATOS

En este apartado se define como eliminar datos desde SQL Server Management Studio.

Paso	Descripción
113.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
114.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 

Paso	Descripción
115.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar". 
116.	Dentro del Explorador de objetos, expanda el árbol "Bases de datos" hasta llegar a la tabla que en la que desea eliminar un dato.  **Nota:** En este ejemplo, se utiliza la tabla "dbo.Clientes".

Paso	Descripción
117.	Una vez seleccionada la tabla, haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Editar las 200 primeras filas" para insertar los datos en la tabla seleccionada. 
118.	Haga clic derecho sobre fila que desea eliminar y pinche sobre la opción del menú contextual "Eliminar" para borrar el registro seleccionado. 

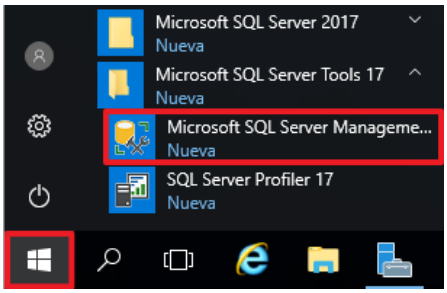
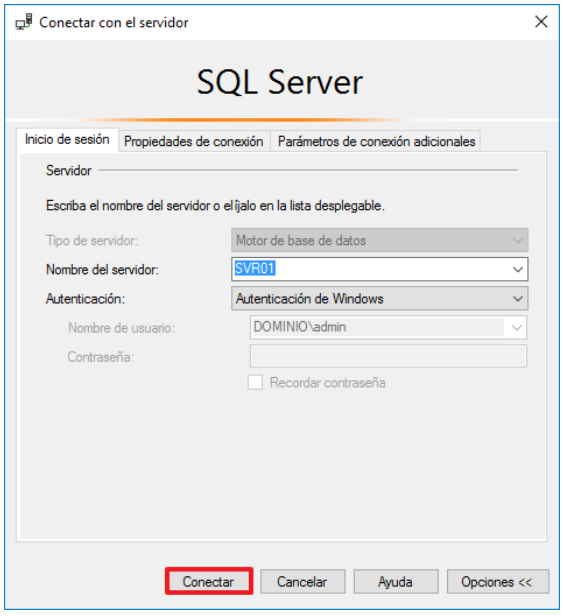
2.5. ASIGNACIÓN DE PERMISOS SOBRE SQL

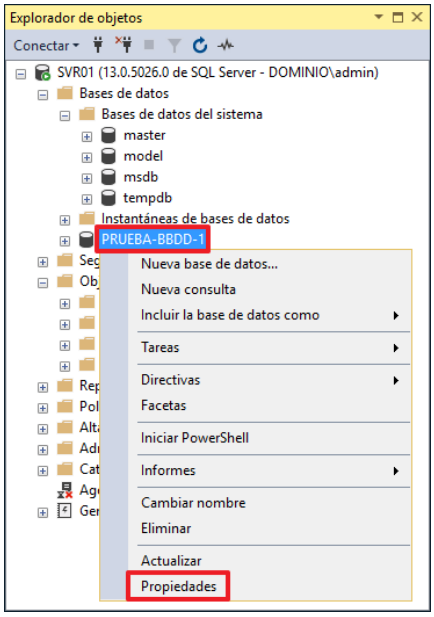
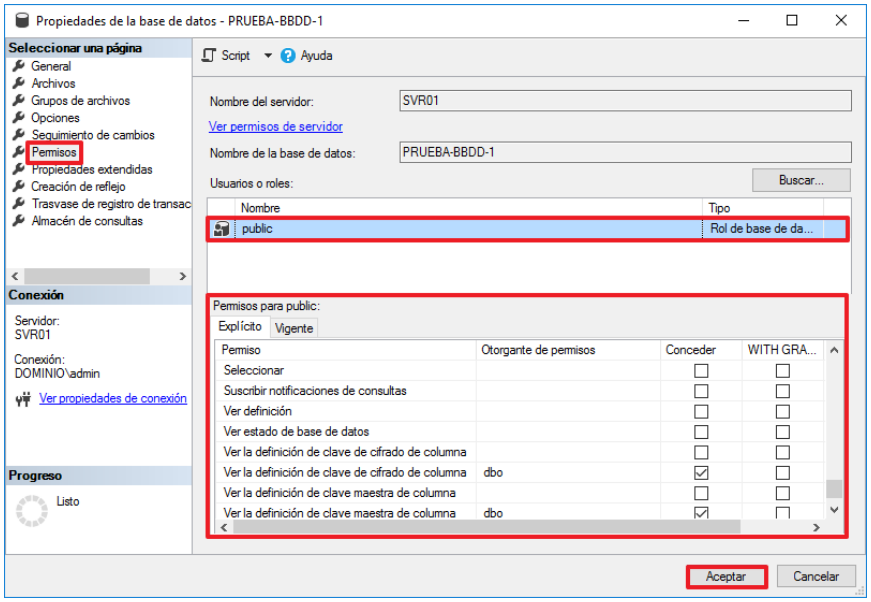
Los permisos de acceso sobre los diferentes datos dentro de SQL Server 2016 debe quedar limitado a los usuarios legitimados para ello. Por lo tanto, será necesario establecer los permisos necesarios para limitar dicho acceso.

2.5.1. PERMISOS EN BASES DE DATOS

En esta sección se definen los procesos para alterar los permisos de los diferentes objetos de la base de datos.

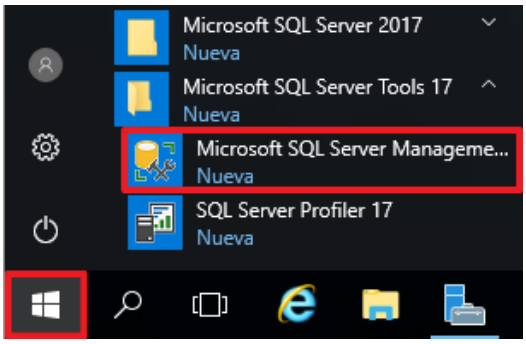
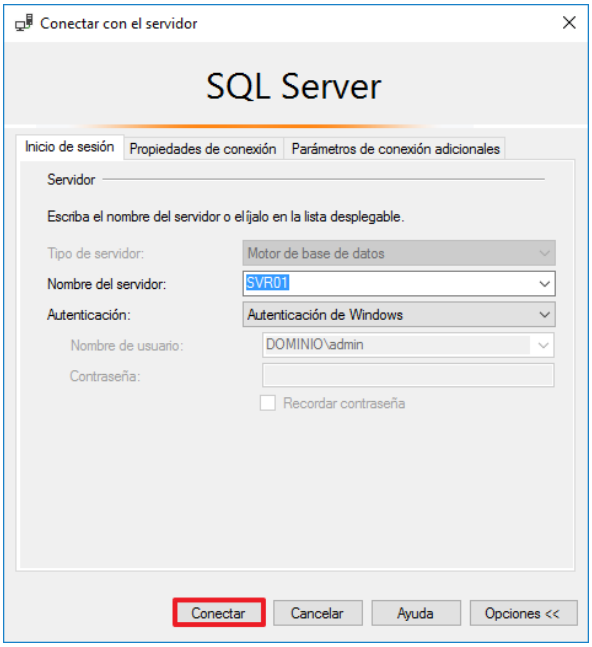
Paso	Descripción
119.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.

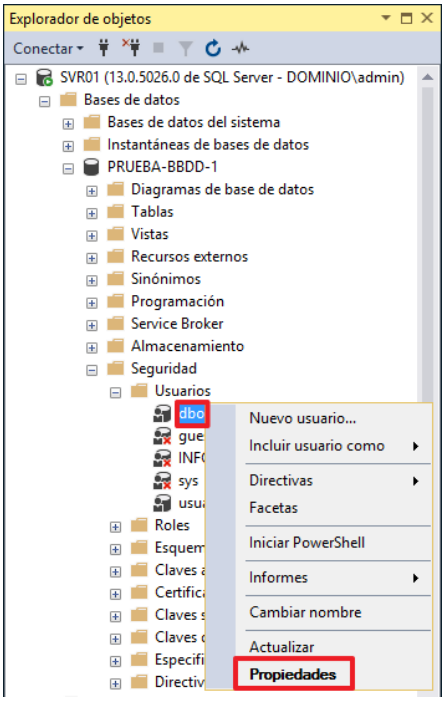
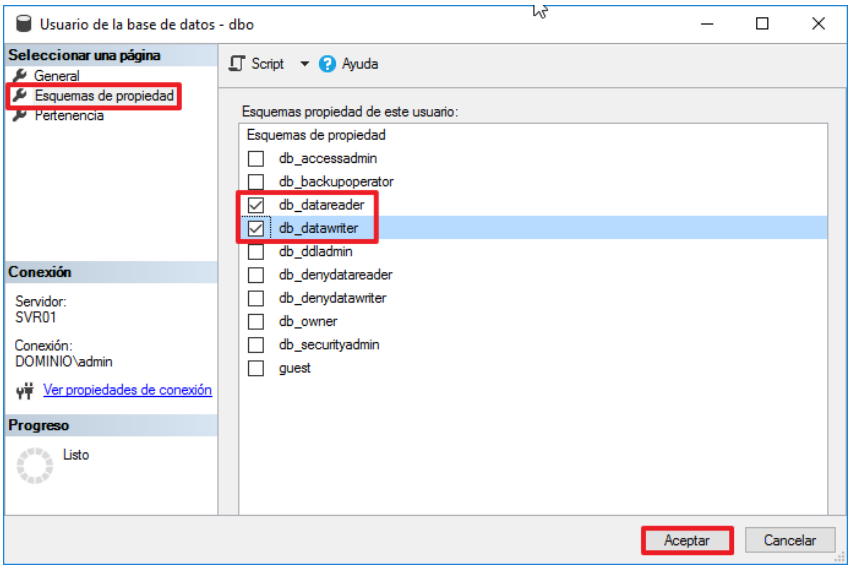
Paso	Descripción
120.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
121.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar". 

Paso	Descripción
122.	Una vez seleccionada la tabla, haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Propiedades".  **Nota:** En este ejemplo, se utiliza la base de datos "PRUEBA-BBDD-1".
123.	En la siguiente pantalla, seleccione en el menú de la izquierda la página "Permisos" y establezca los permisos necesarios a corde a su organización. Cuando haya finalizado pulse "Aceptar" para guardar los permisos configurados.  **Nota:** SQL Server posee una gestión de usuarios, roles, permisos y políticas sobre los objetos específicos contenidos en la base de datos dentro del servidor SQL. Dicha gestión se puede asignar mediante permisos de seguridad individuales para cada uno de estos objetos. Para más información sobre los permios en SQL Server 2016 consulte la siguiente página: https://docs.microsoft.com/es-es/sql/relational-databases/security/permissions-database-engine?view=sql-server-2016.

2.5.2. PERMISOS DE USUARIOS SOBRE BASES DE DATOS

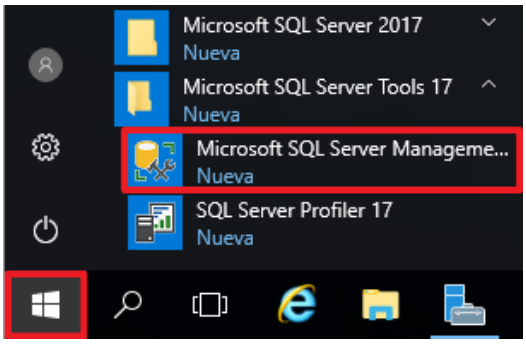
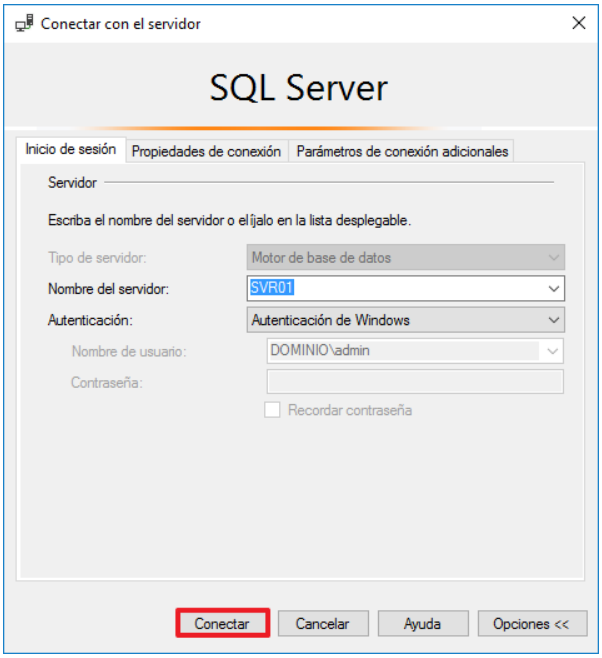
En esta sección se definen los procesos para alterar los permisos de los diferentes usuarios sobre una base de datos.

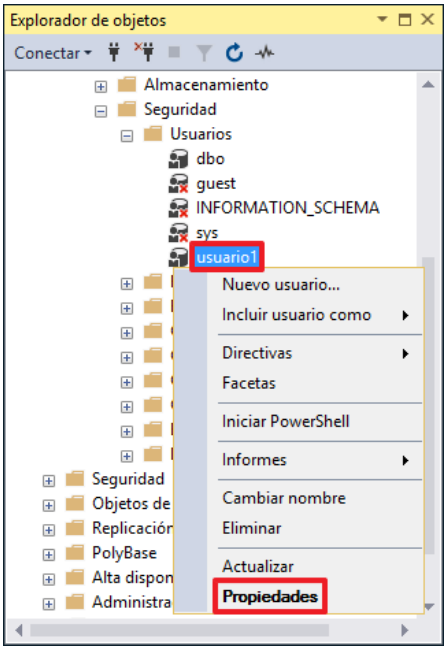
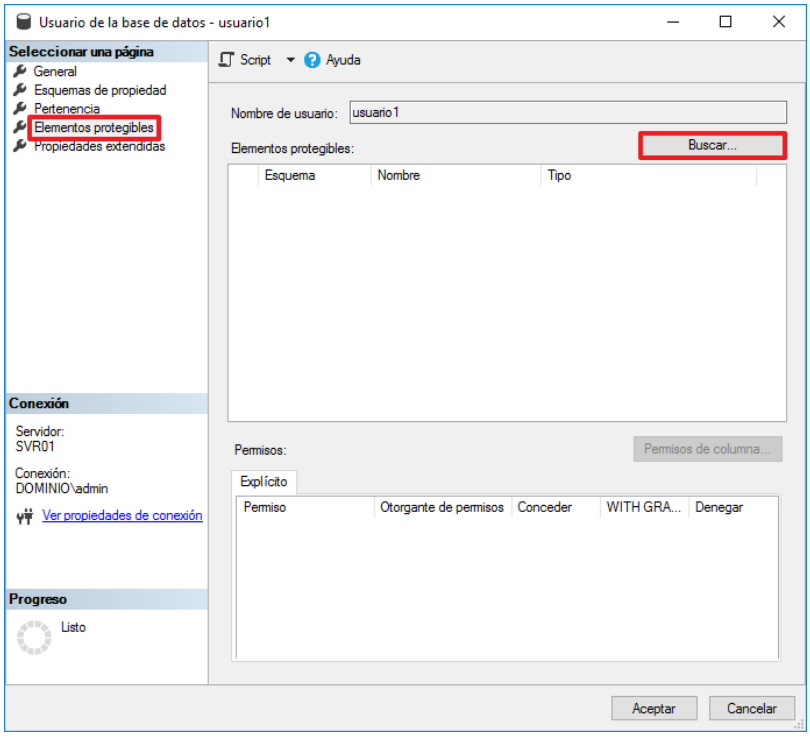
Paso	Descripción
124.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
125.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
126.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar". 

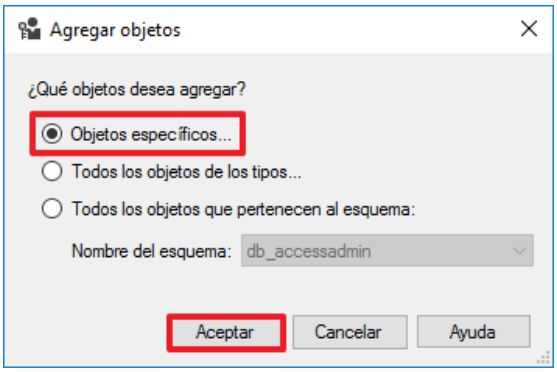
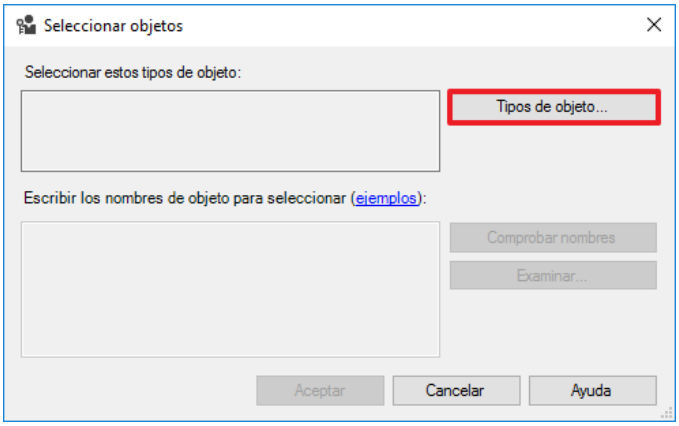
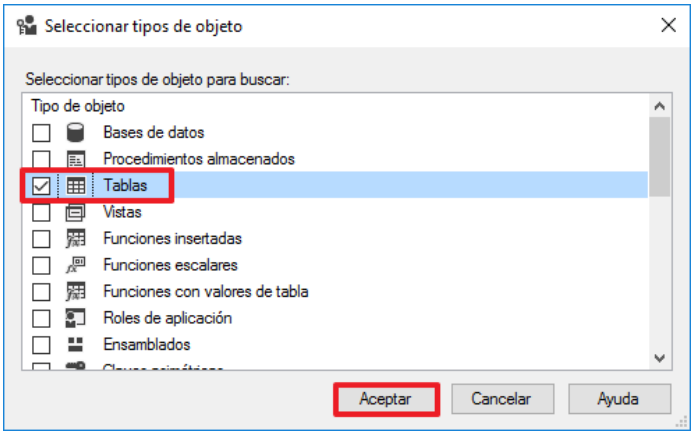
Paso	Descripción
127.	Una vez dentro de la consola de administración de SQL Server, expanda el árbol de su base de datos hasta llegar al siguiente nodo **"Bases de datos → <PRUEBA-BBDD-1> → Seguridad → Usuarios"** y desplegando el menú contextual con el botón derecho sobre el usuario que quiera administrar, seleccione la opción "Propiedades".  **Nota:** En este ejemplo, se utiliza el usuario "dbo" sobre la base de datos "PRUEBA-BBDD-1".
128.	En la siguiente ventana, sitúese en el menú de la izquierda y pinche en la página "Esquemas de propiedad" y asigne los permisos de usuario sobre la base datos acorde a las necesidades de su organización y pulse "Aceptar".  **Nota:** En este ejemplo, se han asignado los permisos de lectura ("db_datareader") y modificación ("db_datawriter").

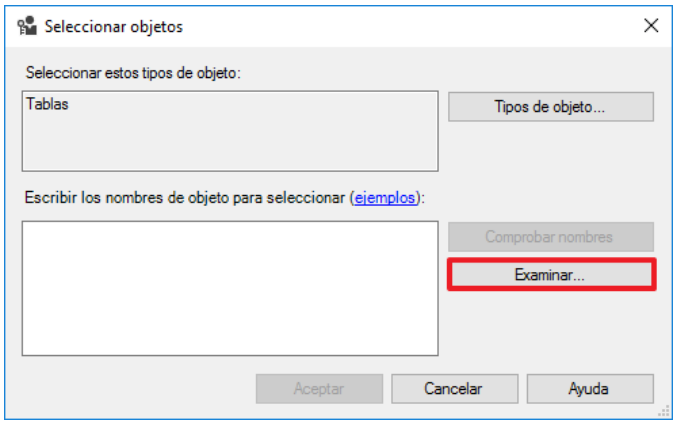
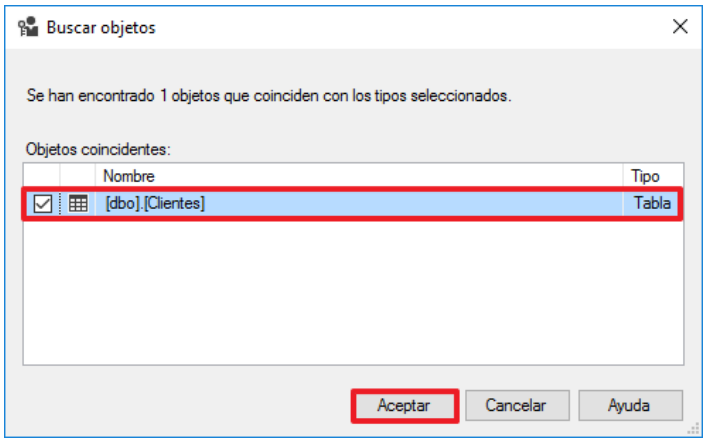
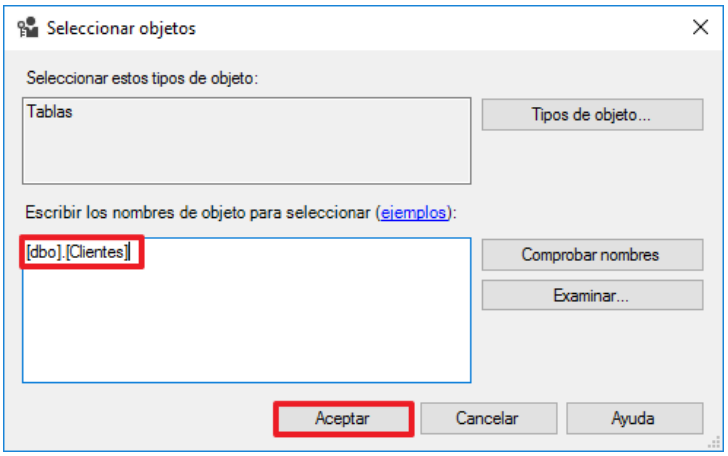
2.5.3. PERMISOS EN TABLAS

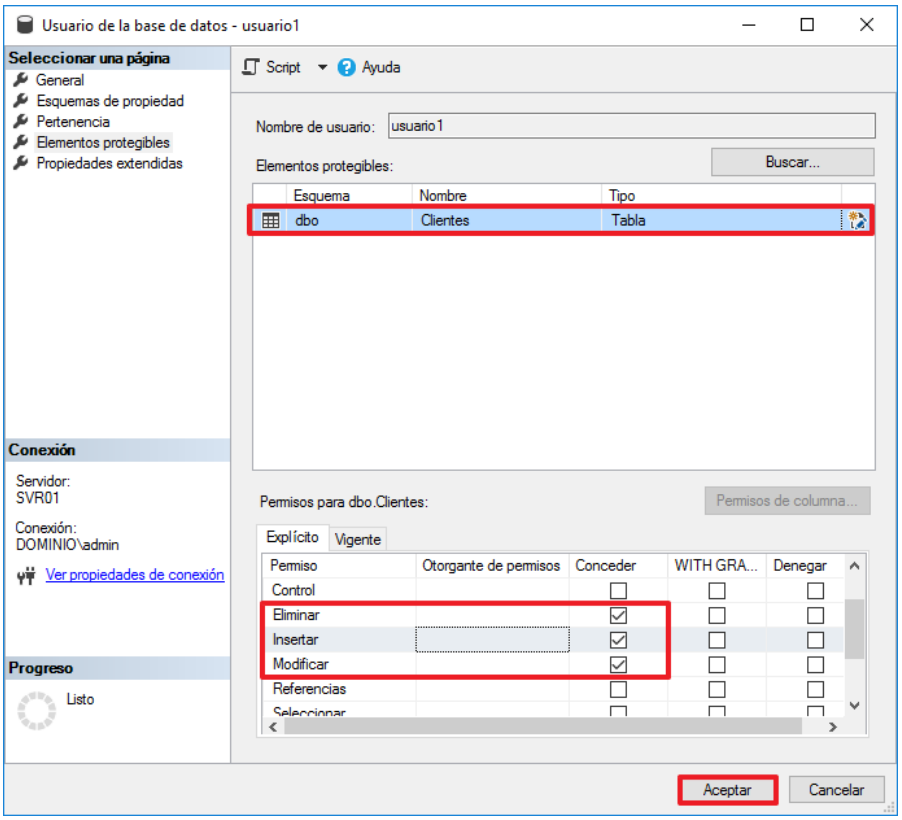
En esta sección se definen los procesos para añadir permisos específicos a un usuario sobre una tabla de una base de datos de SQL Server 2016.

Paso	Descripción
129.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
130.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".** 
131.	En la ventana de "Conectar con el servidor", asegúrese de que el nombre del servidor es el correcto y pulse "Conectar". 

Paso	Descripción
132.	Una vez dentro de la consola de administración de SQL Server, expanda el árbol de su base de datos hasta llegar al siguiente nodo **"Bases de datos → <PRUEBA-BBDD-1> → Seguridad → Usuarios"** y desplegando el menú contextual con el botón derecho sobre el usuario que quiera administrar, seleccione la opción "Propiedades".  **Nota:** En este ejemplo, se utiliza el usuario "usuario1" sobre la base de datos "PRUEBA-BBDD-1".
133.	En la siguiente ventana, sitúese en el menú de la izquierda y pinche en la página "Elementos protegibles" y pulse sobre el botón "Buscar...". 

Paso	Descripción
134.	A continuación, seleccione "Objetos específicos…" y pulse "Aceptar". 
135.	En la siguiente ventana emergente, presione "Tipos de objeto…". 
136.	Seleccione el objeto "Tablas" y pulse "Aceptar". 

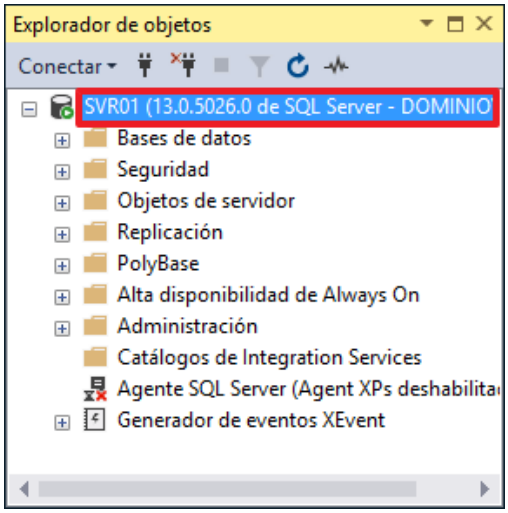
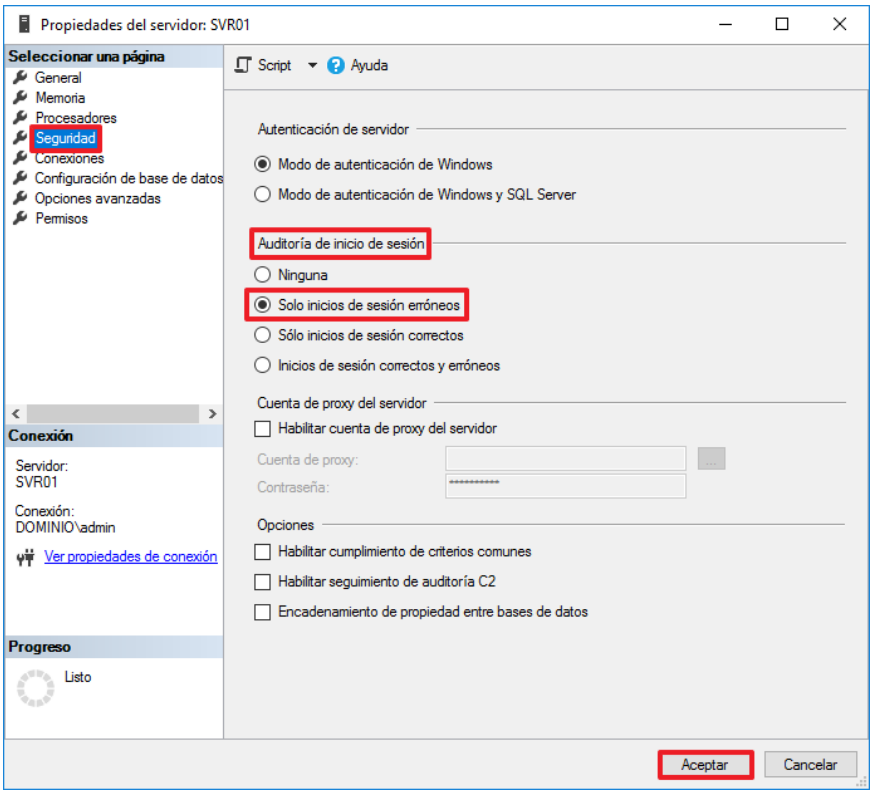
Paso	Descripción
137.	A continuación, pulse el botón "Examinar…". 
138.	En la siguiente ventana emergente, seleccione la tabla que desea asignarle al usuario previamente establecido. 
139.	Para finalizar, compruebe que la tabla se ha asignado correctamente y vuelva a pulsar "Aceptar" para guardar los cambios. 

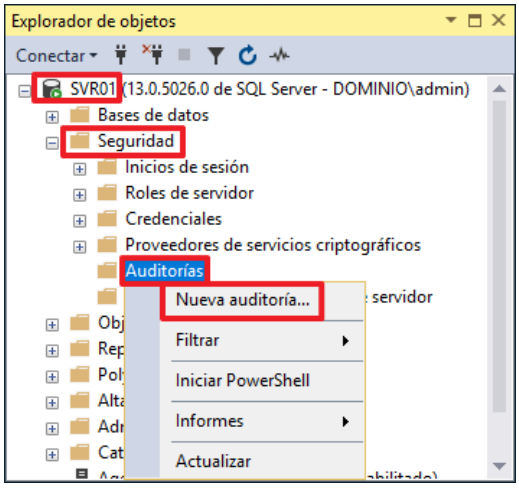
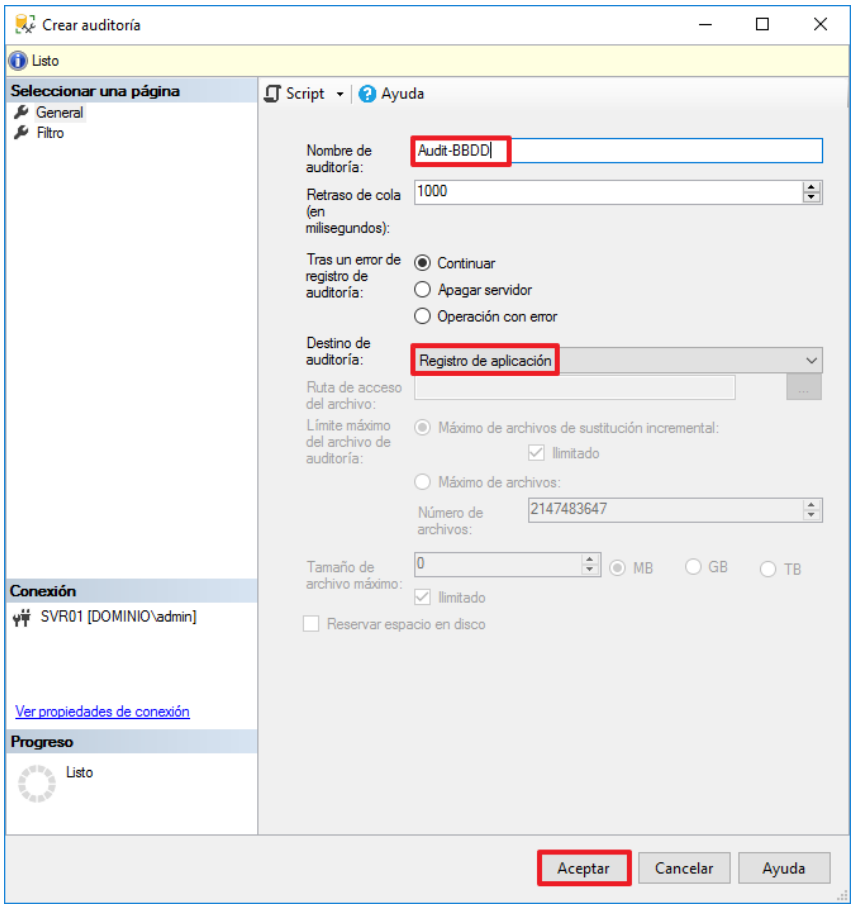
Paso	Descripción
140.	En la parte inferior de la ventana, asigne los permisos al usuario sobre la tabla seleccionada acorde a las necesidades de su organización. Pulse "Aceptar" para guardar los cambios.  **Nota:** En este ejemplo, se han asignado los permisos de eliminar, insertar y modificar al usuario "usuario1" sobre la tabla "Clientes".

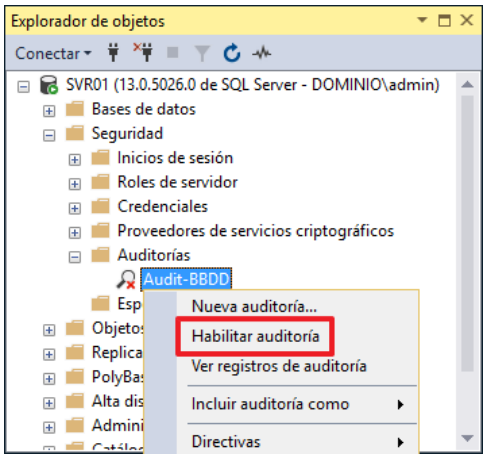
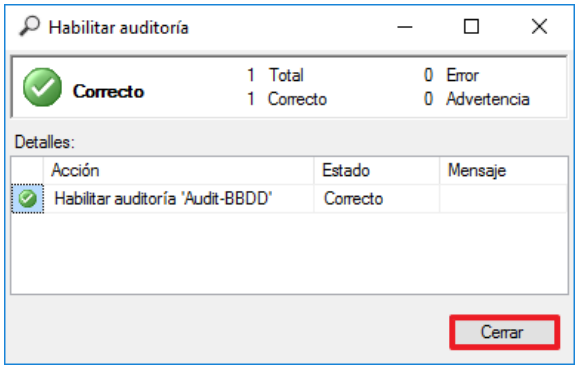
2.6. AUDITORÍA EN SQL SERVER 2016

Existe la posibilidad que auditores lleven un control de las diferentes tareas que se realizan a través de SQL Server 2016. Esta sección recoge los pasos a seguir para realizar la configuración de una auditoria de eventos de un servidor de SQL Server 2016. Estos pasos se realizarán a través de un servidor SQL Server 2016.

Paso	Descripción
141.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
142.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**.
143.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".

Paso	Descripción
144.	Dentro del Explorador de objetos, seleccione su servidor de SQL Server y haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Propiedades". 
145.	En la siguiente pantalla, seleccione en el menú de la izquierda la página "Seguridad" y en el apartado de "Auditoria de inicio de sesión" marque la opción "Solo inicios de sesión erroneos". Cuando haya finalizado pulse "Aceptar" para guardar los permisos configurados. 

Paso	Descripción
146.	A continuación, despliegue el nodo **"Servidor: <<nombre del servidor>> → Seguridad → Auditorías"** y desplegando el menú contextual con el botón derecho, seleccione la opción **"Nueva auditoria"**.  **Nota:** En este ejemplo se utiliza el servidor con el nombre "SVR01".
147.	En la siguiente ventana de auditoria, establezca un nombre para el registro de auditoria y defina el parametro "Registro de aplicación" como destino de auditoria. Pulse "Aceptar" para guardar los cambios.  **Nota:** En este ejemplo se utiliza el nombre de auditoria "Audit-BBDD".

Paso	Descripción
148.	Ahora, seleccione la auditoria recien creda y desplegando el menú contextual con el botón derecho, seleccione la opción "Habilitar auditoria". 
149.	Una vez finalizado el proceso, verifique que el estado de la acción sea correcto y pulse "Cerrar". 

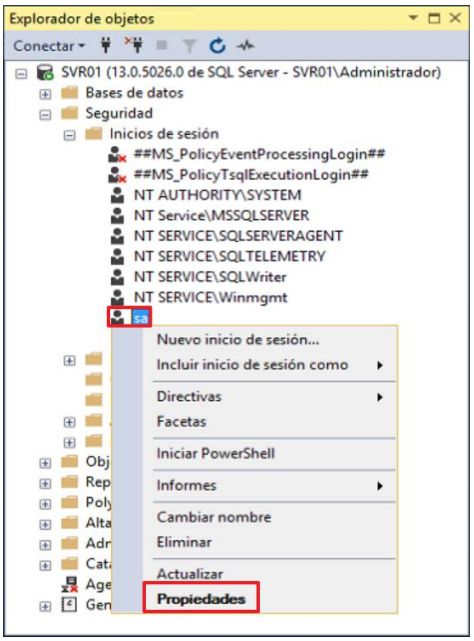
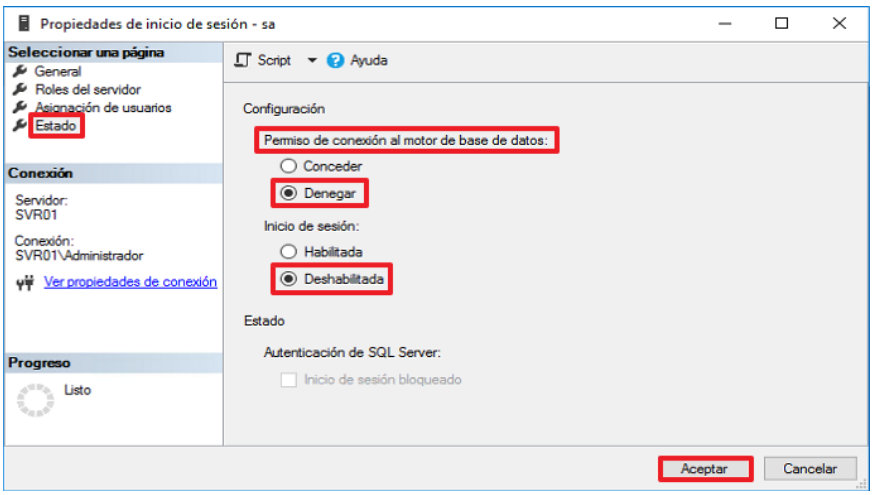
2.7. SEGURIDAD SOBRE EL USUARIO SA

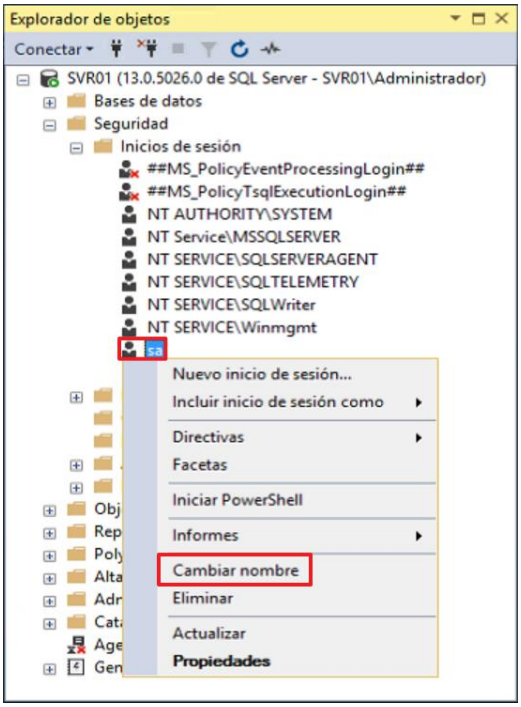
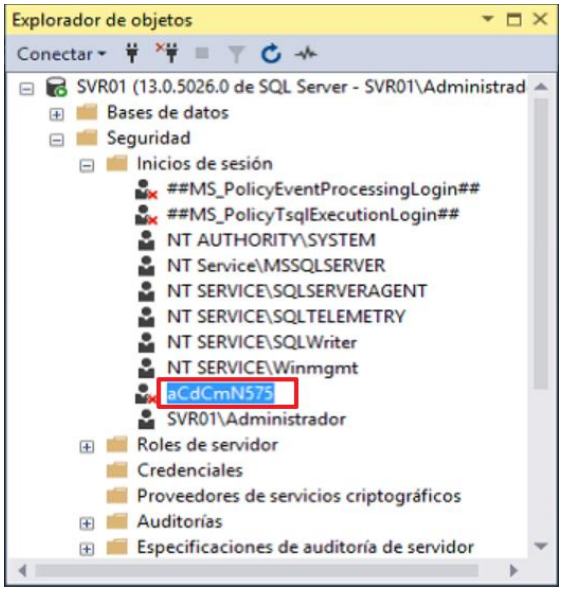
SQL Server 2016 instala de forma predeterminada un inicio de sesión denominado "sa" como abreviatura de "system administrator" ("administrador de sistema"). El inicio de sesión de "sa" se asigna al rol del servidor sysadmin, que dispone de credenciales administrativas irrevocables en todo el servidor.

Para ello, en el siguiente punto se deshabilitará el inicio de sesión del usuario "sa" y se le asignará un nombre alternativo para impedir ataques de fuerza bruta sobre dicho usuario.

Nota: Antes de empezar, asegúrese de tener al menos una cuenta perteneciente al rol del servidor de "Sysadmin".

Paso	Descripción
150.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.

Paso	Descripción
151.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".**
152.	En la ventana de "Conectar con el servidor", asegúrese de que el nombre del servidor es el correcto y pulse "Conectar".
153.	A continuación, despliegue el nodo **"Servidor: <<nombre del servidor>> → Seguridad → Inicios de sesión"** y desplegando el menú contextual con el botón derecho, seleccione la opción "Propiedades".  **Nota:** En este ejemplo, se utiliza el nombre del servidor "SVR01".
154.	A continuación, sitúese en la página "Estado" dentro de la configuración "Permiso de conexión al motor de base de datos" y seleccione "Denegar". Repita el mismo proceso en la configuración "Inicio de sesión" marcando la opción "Deshabilitada". Pulse "Aceptar" para guardar los cambios. 

Paso	Descripción
155.	Una vez deshabilitado el usuario "sa", haga clic derecho sobre dicho usuario y desplegando el menú contextual, seleccione la opción "Cambiar nombre".  **Nota:** Verifique que el usuario "sa" aparece deshabilitado mediante una "X" de color rojo. Si no es así, pulse F5 para refrescar el explorador de objetos.
156.	Establezca el nombre "aCdCmN575" para el usuario "sa". 

ANEXO A.2.2. LISTA DE COMPROBACIÓN DE SQL SERVER 2016 SOBRE WINDOWS SERVER 2016 PARA SERVIDORES QUE LES SON 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 para SQL Server 2016 sobre Microsoft Windows Server 2016 con implementación de seguridad de categoría básica 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 la sección de la guía "ANEXO A.2.1 PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE MS SQL SERVER 2016 SOBRE SERVIDORES WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS.

1. COMPROBACIONES EN CONTROLADOR DE DOMINIO

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

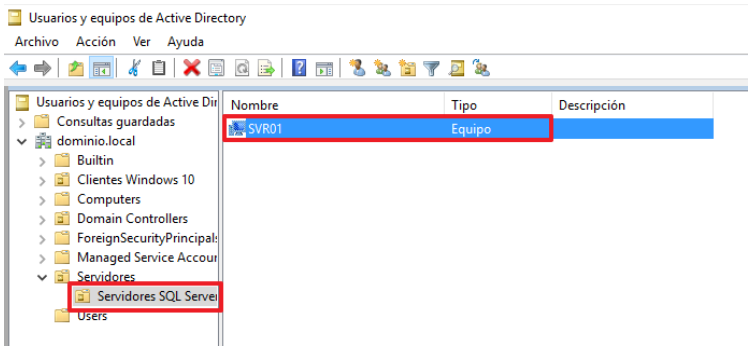
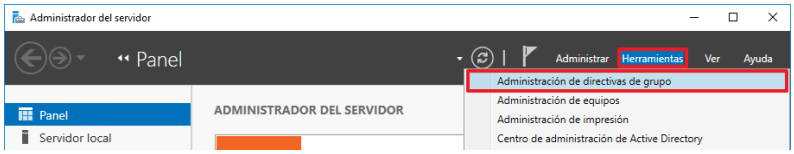
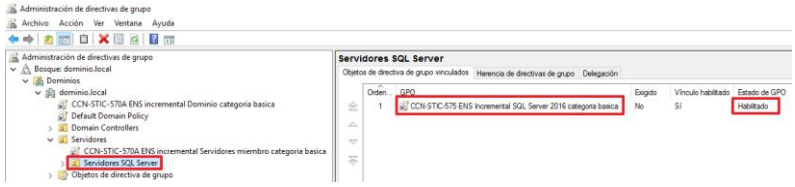
a) Usuarios y equipos de Active Directory (dsa.msc).

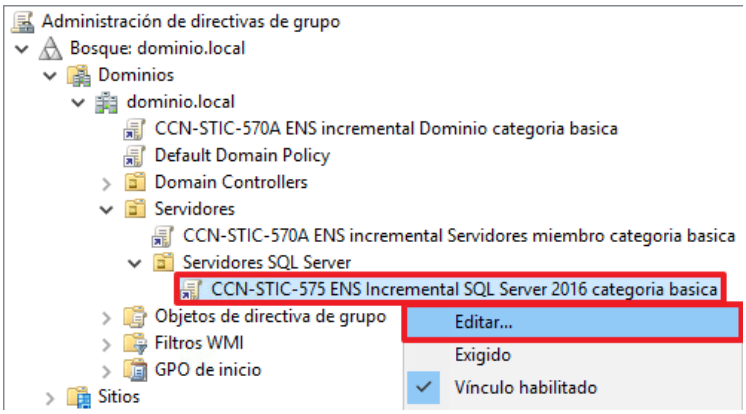
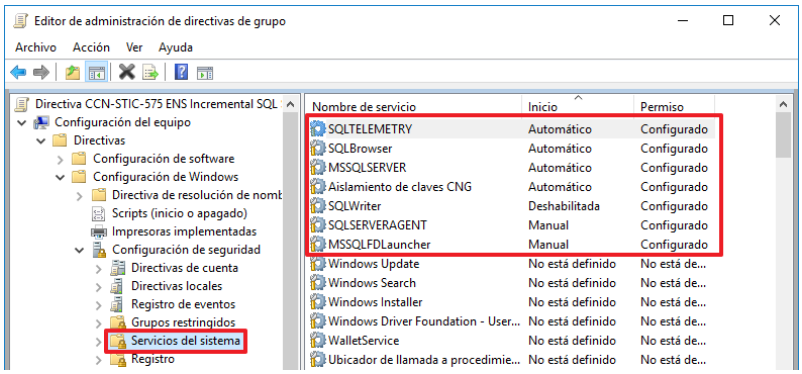
b) Administrador de directivas de grupo (gpmc.msc).

c) Editor de objetos de directiva de grupo (gpedit.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 el servidor 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 los servidores que tienen SQL Server instalado están dentro del contenedor "Servidores SQL Server".		Utilizando la consola de "Usuarios y Equipos de Directorio Activo" **(Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory).** Seleccione la unidad organizativa "**Servidores → Servidores SQL Server**", y verifique que existe un objeto de tipo "Equipo" que corresponde al servidor donde se ha instalado SQL Server 2016.  **Nota:** En este ejemplo se ha utilizado la cuenta de equipo SVR01. En otra organización los nombres pueden variar.
3. Verifique que los objetos de directivas de grupo han sido creados y están habilitados.		Ejecute la herramienta "Administrador de directivas de grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: "**Herramientas → Administración de directivas de grupo**"  Dentro de la consola diríjase a los "Objetos de directiva de grupo": "**Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo**" Verifique que está creado el objeto de directiva de grupo "CCN-STIC-575 ENS Incremental SQL Server 2016 categoria basica" y que en la columna "Estado de GPO" figura como habilitado. 

Comprobación	OK/NOK	Cómo hacerlo
4. Verifique los servicios del sistema de la directiva SQL Server (CCN-STIC-575 Incremental SQL Server 2016 categoria basica).		Seleccionando dicha directiva, pinche sobre ella con el botón derecho y seleccione la opción "Editar" del menú contextual, se abrirá la herramienta "Editor de administración de directiva de grupo" que permitirá verificar los valores de la directiva "CCN-STIC-575 ENS Incremental SQL Server 2016 categoria basica".  Verifique que la directiva tiene los siguientes valores en servicios del sistema. Para ello, navegue hasta: **"Directiva CCN-STIC-575 ENS Incremental SQL Server 2016 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
Aislamiento de claves CNG	KeyIso	Automático	Configurado	
SQL Server (MSQLSERVER)	MSSQLSERVER	Automático	Configurado	
SQL Server Browser	SQLBrowser	Automático	Configurado	
SQL Server CEIP service (MSSQLSERVER)	SQLTELEMETRY	Automático	Configurado	
SQL Server VSS Writer	SQLWriter	Deshabilitado	Configurado	
SQL Full-Text Filter Daemon Launcher	MSSQLFDLauncher	Manual	Configurado	
Agente SQL Server (MSSQLSERVER)	SQLSERVERAGENT	Manual	Configurado	

2. COMPROBACIONES EN EL SERVIDOR SQL SERVER 2016

Para realizar esta lista de comprobación primero deberá iniciar sesión en un servidor miembro de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

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

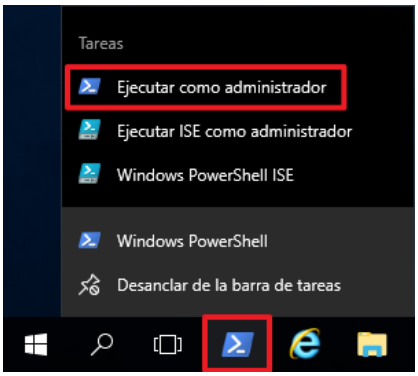
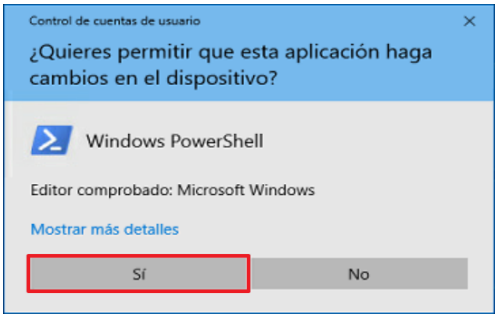
Las consolas y herramientas que se utilizarán son las siguientes:

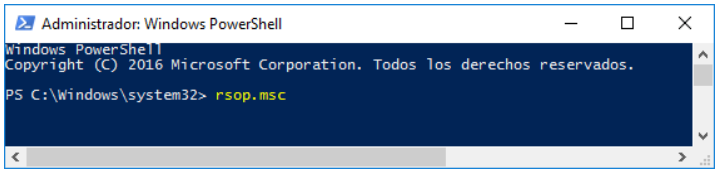
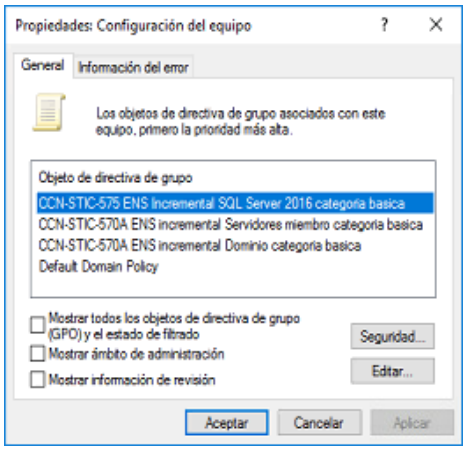
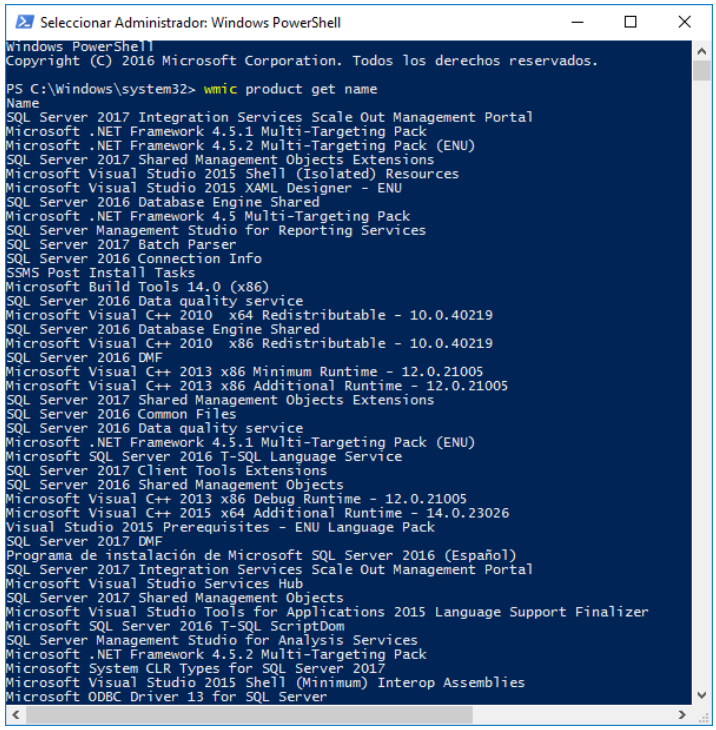
a) Conjunto resultante de directivas (rsop.msc).

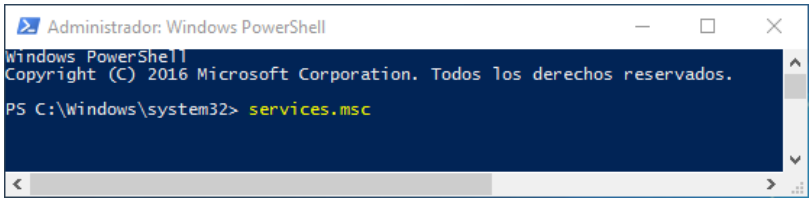
b) Servicios (services.msc).

c) Consola "SQL Server Management Studio".

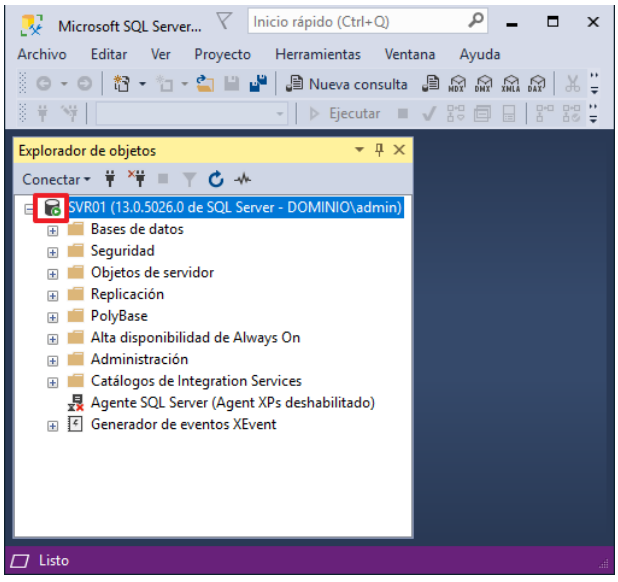
d) Consola "Administrador de configuración de SQL Server".

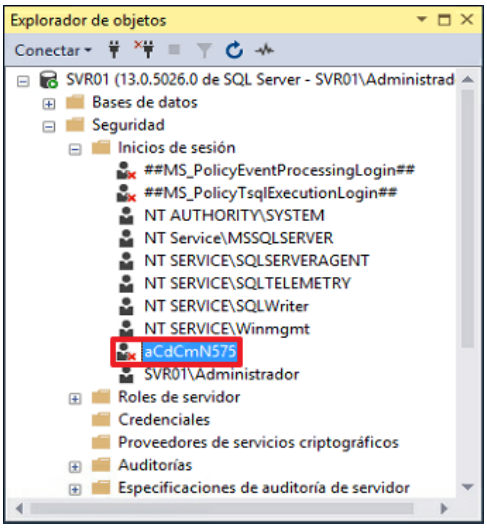
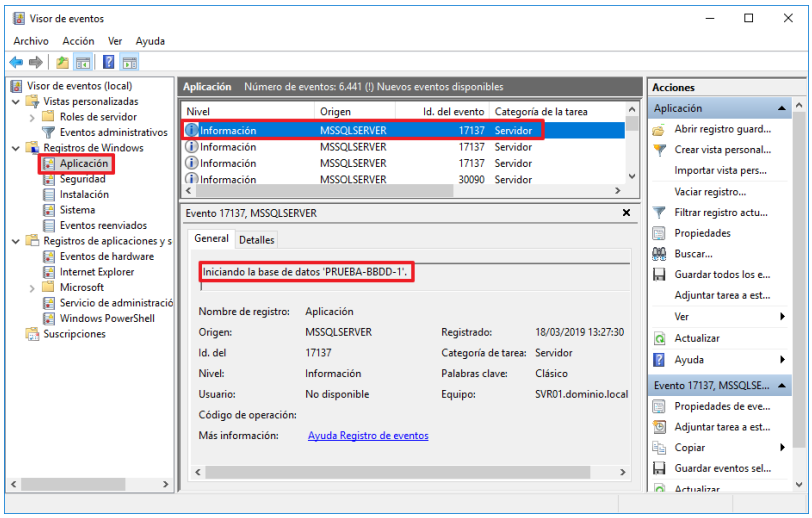
Comprobación	OK/NOK	Cómo hacerlo
5. Inicie sesión en el servidor de SQL Server 2016.		Inicie sesión en el servidor donde se ha implementado el servicio de Microsoft SQL Server 2016 con una cuenta que tenga privilegios de administración del dominio
6. Verifique la correcta aplicación de la política "CCN-STIC-575 Incremental SQL Server 2016 categoria basica" en un equipo miembro del dominio.		Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen.  El sistema solicitará elevación de privilegios para poder ejecutar una sesión de PowerShell como administrador. Pulse "Sí" en la ventana de "Control de cuentas de usuario". 

Comprobación	OK/NOK	Cómo hacerlo
		Teclee rsop.msc en la consola de comandos que se ha abierto.  A continuación, haga clic derecho sobre "Configuración de equipo" en la consola de "Conjunto resultante de directivas" y compruebe que la política "CCN-STIC-575 Incremental SQL Server 2016 categoria basica" aparece en la lista como muestra la imagen. 
7. Verifique que SQL Server se ha instalado correctamente		Teclee "Wmic Product Get Name" en la consola de comandos que se ha abierto anteriormente, y compruebe que aparecen al menos los siguientes productos de SQL Server que se muestran en la siguiente imagen. 

Comprobación	OK/NOK	Cómo hacerlo
8. Verifique la correcta aplicación de la configuración de servicios del sistema de la política "CCN-STIC-575 Incremental SQL Server 2016 categoria basica".		Teclee "services.msc" en la consola de comandos que se ha abierto anteriormente:  En la consola de "Servicios", compruebe los siguientes valores.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Aislamiento de claves CNG	KeyIso	Automático	Configurado	
SQL Server (MSQLSERVER)	MSSQLSERVER	Automático	Configurado	
SQL Server Browser	SQLBrowser	Automático	Configurado	
SQL Server CEIP service (MSSQLSERVER)	SQLTELEMETRY	Automático	Configurado	
SQL Server VSS Writer	SQLWriter	Deshabilitado	Configurado	
SQL Full-Text Filter Daemon Launcher	MSSQLFDLauncher	Manual	Configurado	
Agente SQL Server (MSSQLSERVER)	SQLSERVERAGENT	Manual	Configurado	

9. Verifique la conexión con el servicio de SQL Server desde la consola de administración.		Utilizando la consola de administración de SQL Server Management 17 (**"Inicio → Microsoft SQL Server Tools 17 → SQL Server Management Studio 17"**). Compruebe que se puede conectar correctamente al nombre del servidor que ejecuta el motor de bases de datos de SQL Server.  **Nota:** En este ejemplo se utiliza el nombre "SVR01.dominio.local".

Comprobación	OK/NOK	Cómo hacerlo
10. Verifique que el usuario "sa" se encuentra deshabilitado.		Dentro del Explorador de archivos, despliegue el nodo **"Servidor: <<nombre del servidor>> → Seguridad → Inicios de sesión"** y compruebe que el usuario "sa", previamente renombrado como "aCdCmN575", se encuentra deshabilitado. 
11. Verifique que la auditoría sobre el servidor de SQL Server 2016 se encuentra activada		Utilizando la herramienta de visor de eventos de Windows (ejecutando "eventvwr.msc" desde **Inicio → Ejecutar…**), verifique que la auditoría del servidor del servidor de SQL Server 2016 se encuentra activada en el registro de Aplicación. 

ANEXO A.3. CATEGORÍA MEDIA

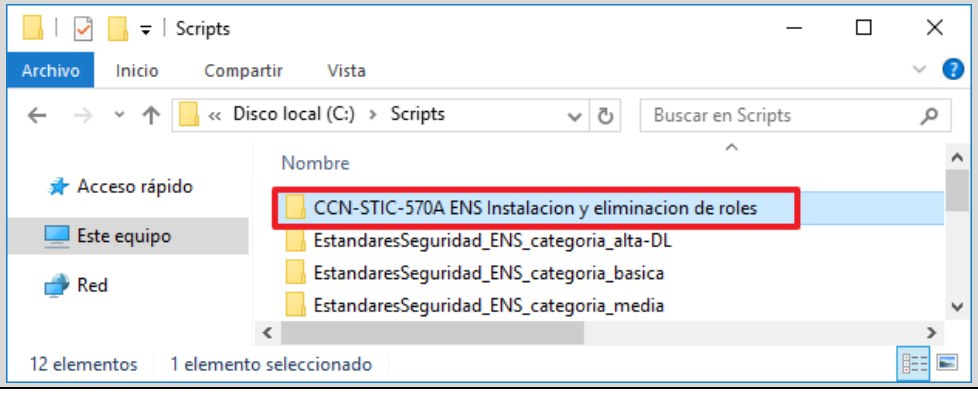
ANEXO A.3.1. PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE MS SQL SERVER 2016 SOBRE SERVIDORES WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

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 SQL Server 2016 con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad.

Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar 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.

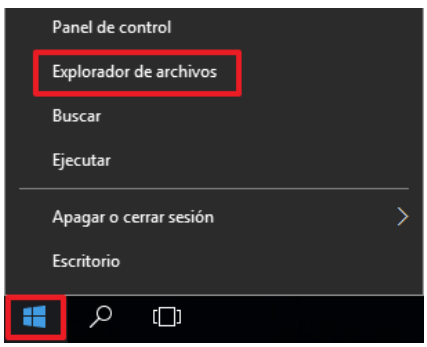
Nota: Si instala SQL Server 2016 por primera vez con la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016 aplicada debe habilitar la instalación remota de roles características y servicios de rol a través de Shell la cual se encuentra deshabilitada por GPO.
En la guía mencionada anteriormente 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.

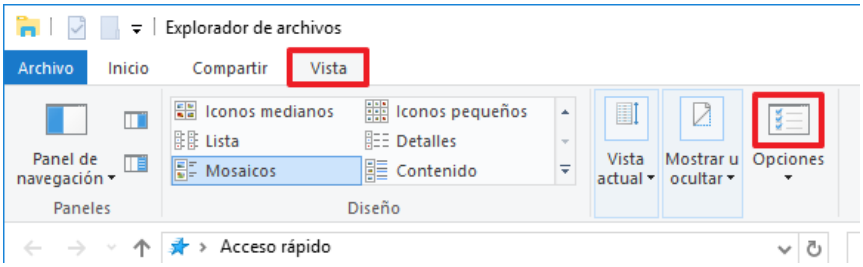
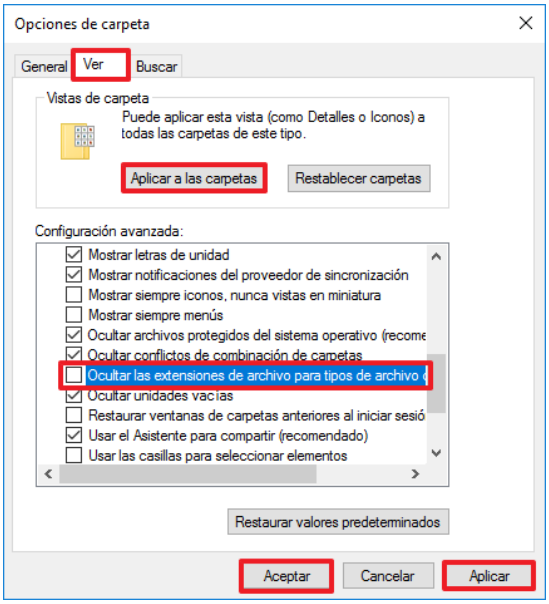
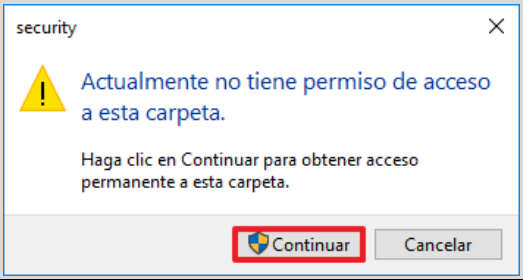


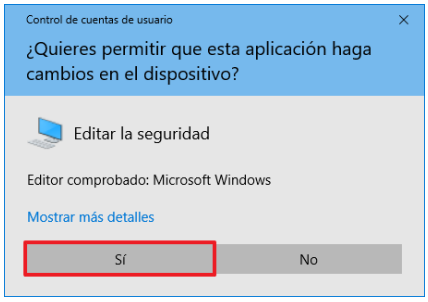
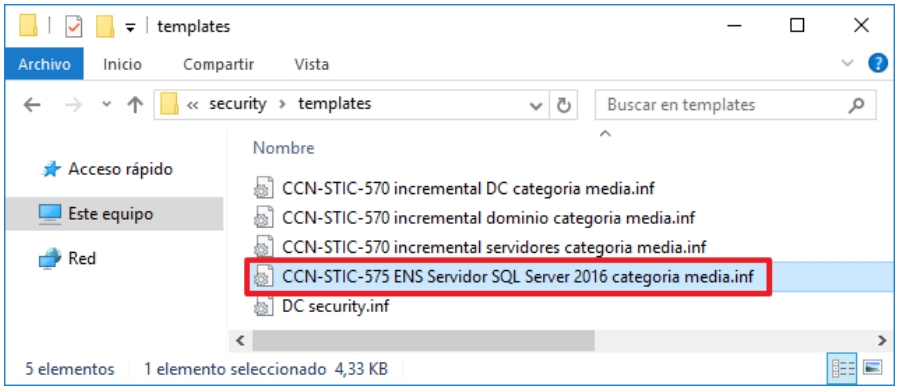
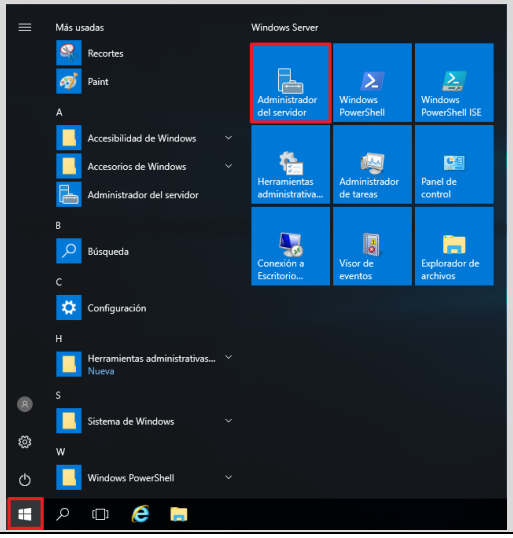
1. PREPARACIÓN DEL DOMINIO

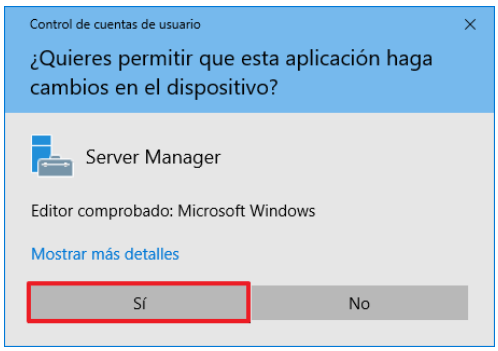
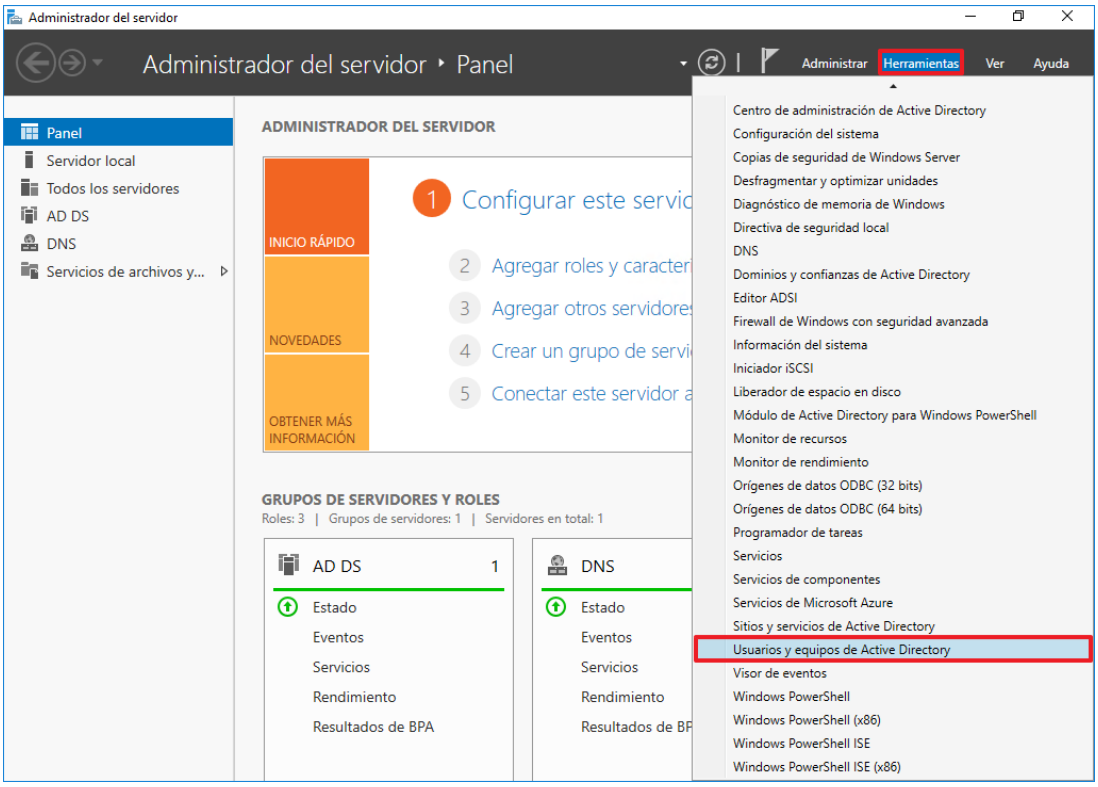
Los pasos que se describen a continuación deberá realizarlos en un Controlador de Dominio del dominio al que pertenece el equipo servidor que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer servidor de SQL Server 2016 que actúe como miembro del dominio. Durante este procedimiento se crea la unidad organizativa que contiene los servidores de SQL Server y se realizan las configuraciones de políticas de grupo correspondientes.

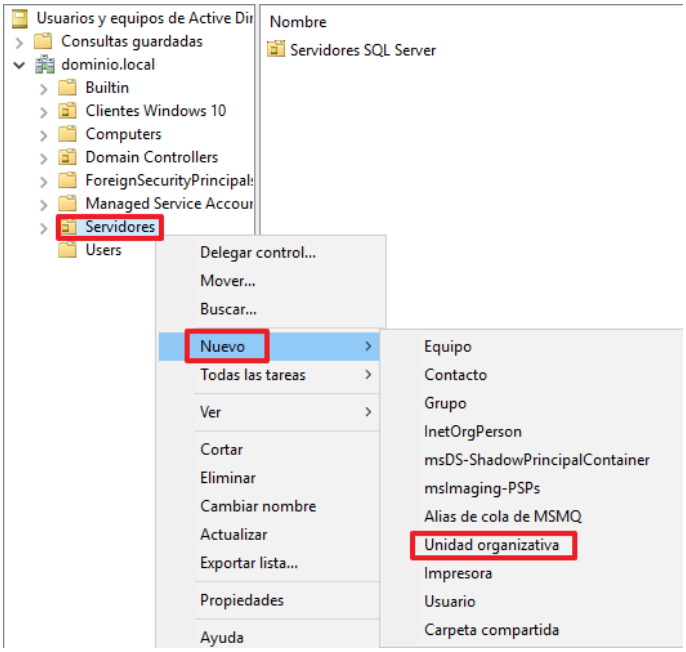
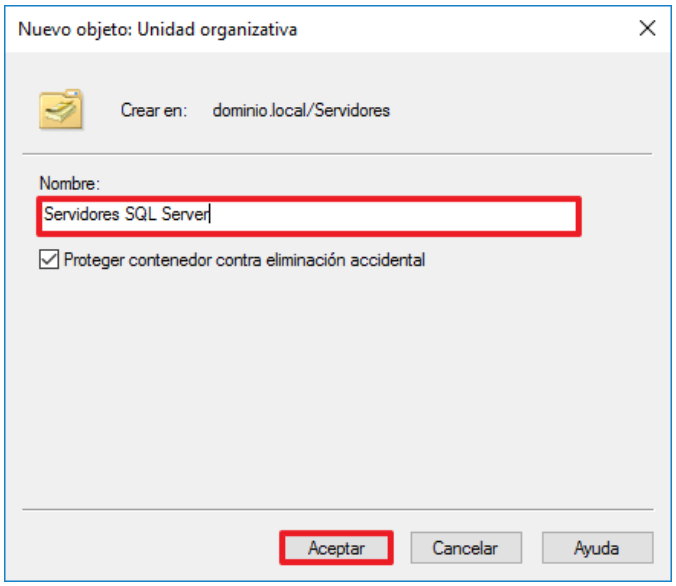
Nota: Esta guía asume que los servidores Controladores del Dominio al que pertenece el equipo servidor de SQL Server 2016 que está asegurando, se les ha aplicado la configuración descrita en la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016". Si no es así, aplique la guía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

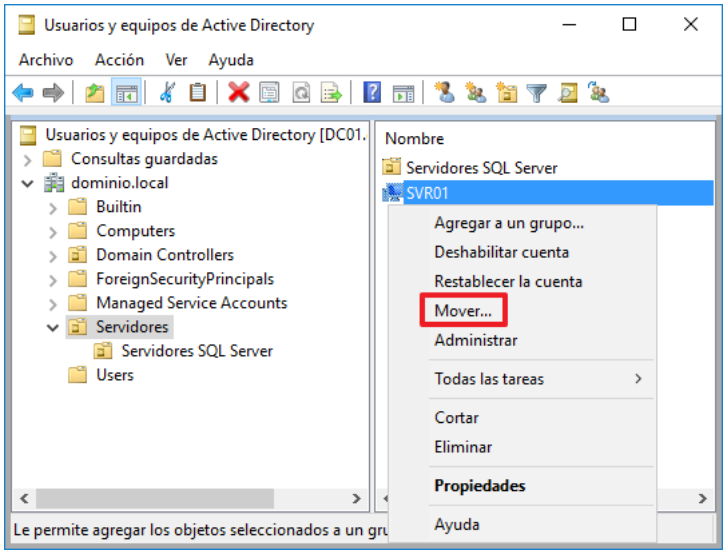
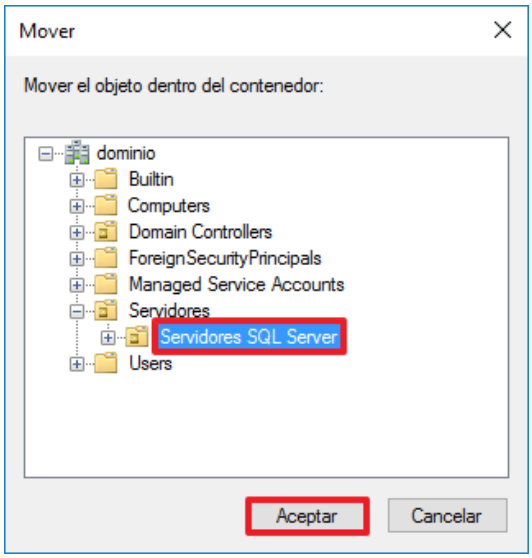
Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio del dominio donde se va a aplicar seguridad para el servidor SQL Server 2016 según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
2.	Cree el directorio "Scripts" en la unidad "C:\". **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. 

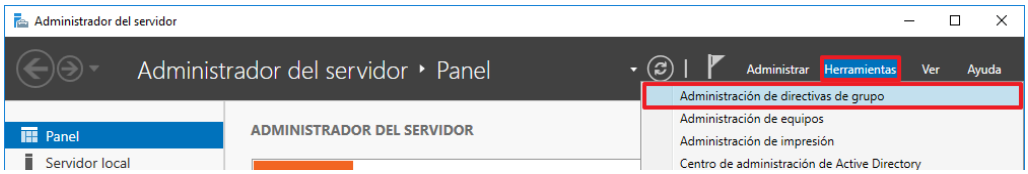
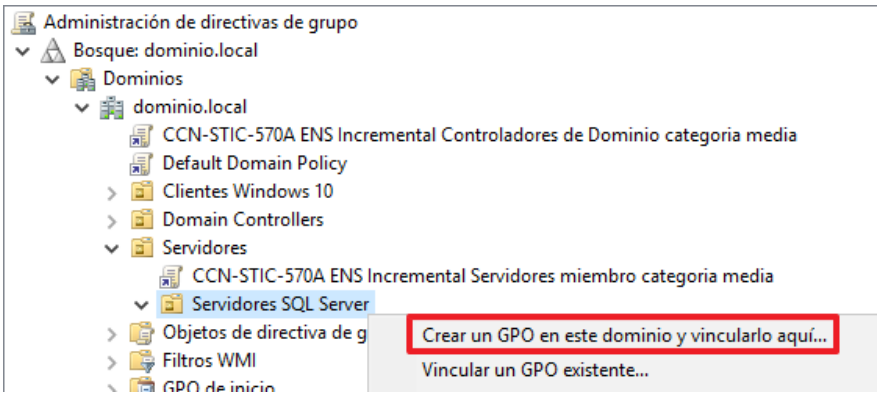
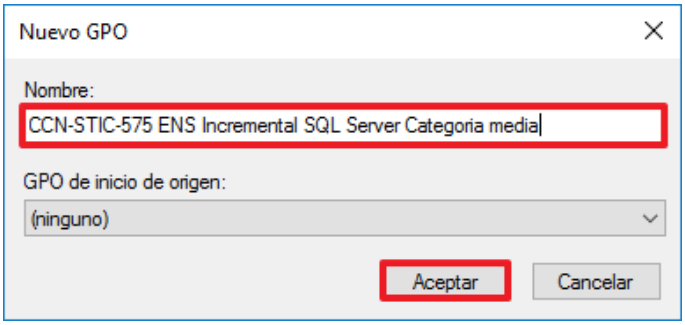
Paso	Descripción
5.	En el "Explorador de archivos" pulse sobre la pestaña "Vista" del menú superior y seleccione el icono de "Opciones". 
6.	En "Opciones de carpeta" sitúese en la pestaña "Ver" y en el campo "Configuración avanzada" localice y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos". Pulse primero sobre el botón "Aplicar", después sobre "Aplicar a las carpetas" (Pulse "Sí" ante el mensaje de confirmación) y, por último, pulse "Aceptar". 
7.	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. 

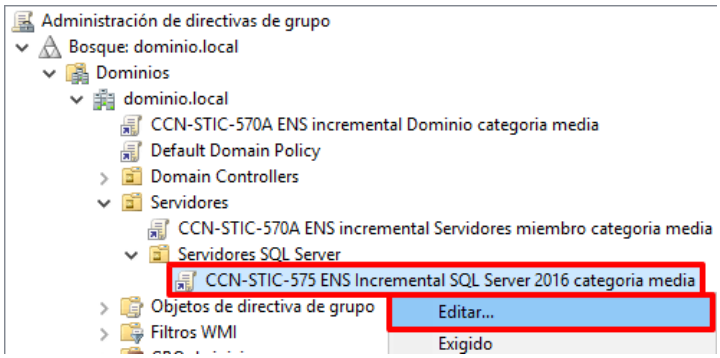
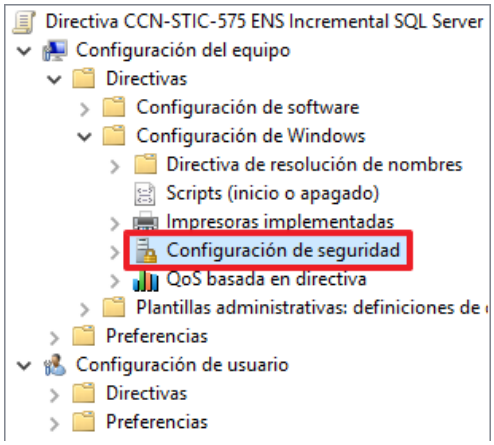
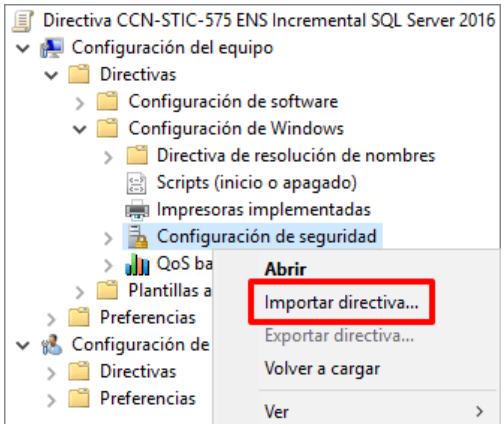
Paso	Descripción
8.	El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse "Sí" para continuar. 
9.	Copie el fichero "CCN-STIC-575 ENS Servidor SQL Server 2016 categoria media.inf" al directorio "%SYSTEMROOT%\Security\Templates" del Controlador de Dominio. 
10.	A continuación, abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas.  **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"**. 

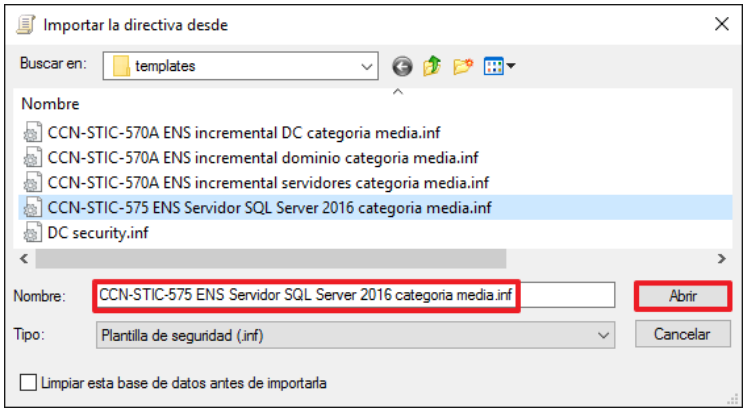
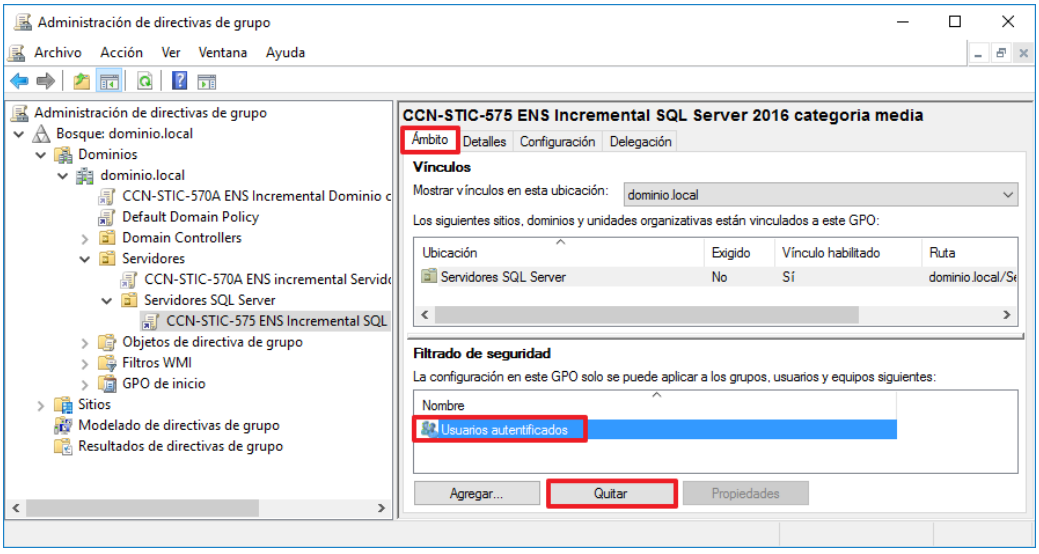
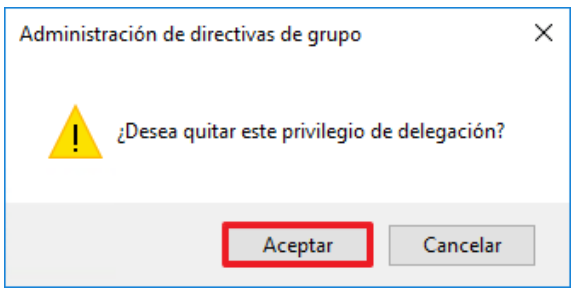
Paso	Descripción
11.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
12.	Inicie la herramienta de usuarios y equipos del Directorio Activo. Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione **"Herramientas → Usuarios y equipos de Active Directory"**. 

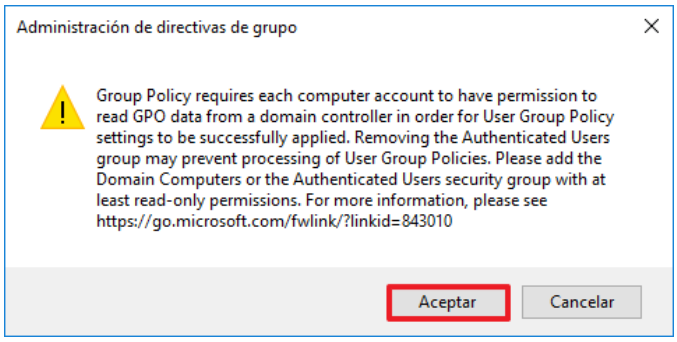
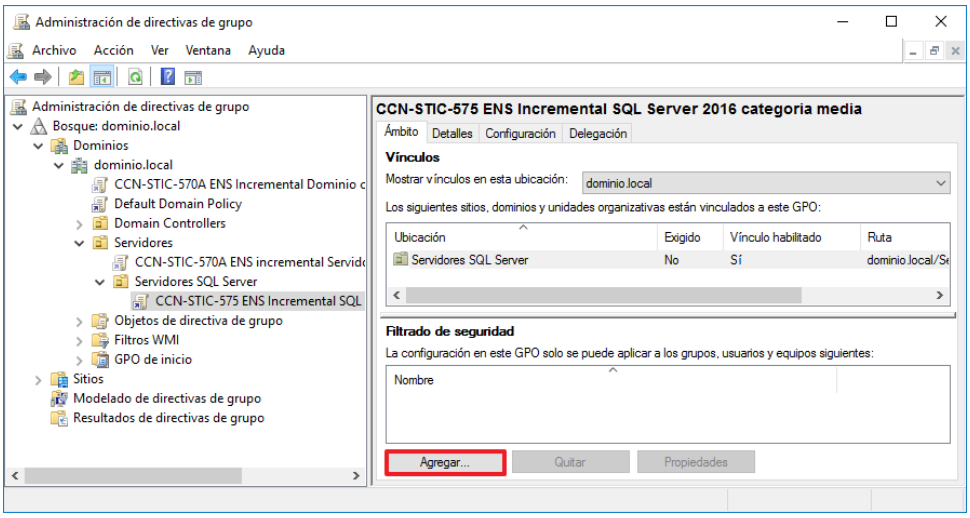
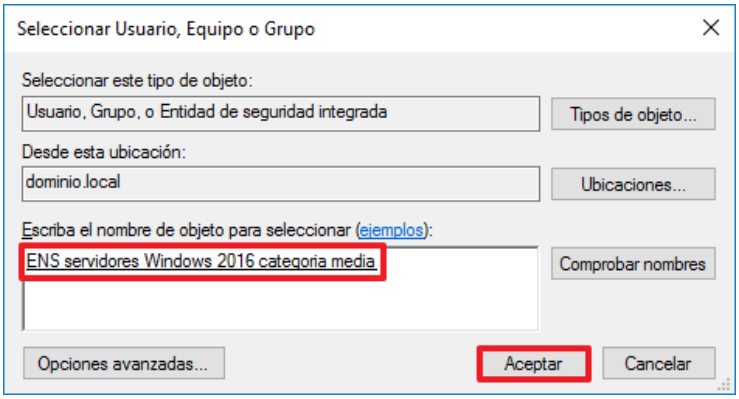
Paso	Descripción
13.	En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo **"<<dominio>> → <<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 **"dominio.local/servidores".**
14.	Introduzca el nombre "Servidores SQL Server" tal y como se muestra en la imagen y pulse sobre "Aceptar".  **Nota:** Puede establecer el nombre que más se adecúe a las necesidades de su organización.

Paso	Descripción
15.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores de virtualización a la unidad organizativa "Servidores de SQL Server". Para ello, haga clic con el botón derecho sobre el equipo que desee reubicar y seleccione la opción del menú contextual "Mover...". 
16.	A continuación, seleccione la unidad organizativa "Servidores de SQL Server" y pulse sobre "Aceptar". 
17.	Cierre la herramienta "Usuarios y equipos de Active Directory".
18.	A continuación, deberá crear la GPO "CCN-STIC-575 ENS incremental Servidor de SQL Server categoria media". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 

Paso	Descripción
19.	Inicie la herramienta "Administración de Directivas de Grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"**. 
20.	A continuación, despliegue el nodo **"Bosque: <<nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores SQL Server"**. **Nota:** En este ejemplo el nombre de la unidad organizativa donde se encuentran todos los servidores que implementan este rol, "Servidores SQL Server".
21.	Pulse con el botón derecho sobre la unidad organizativa "Servidores de SQL Server" y seleccione "Crear un GPO en este dominio y vincularlo aquí…". 
22.	Introduzca el nombre del objeto GPO, "CCN-STIC-575 ENS Incremental SQL Server 2016 categoria media" y haga clic en el botón "Aceptar". 

Paso	Descripción
23.	Seleccione la directiva recién creada "CCN-STIC-575 ENS Incremental SQL Server 2016 categoria media". Se mostrará una ventana de aviso de la Consola de administración de directivas de grupo, informando que los cambios realizados son globales para la GPO y estos afectarán a todas las ubicaciones en las que se vincule esta GPO. Pulse "Aceptar" este mensaje y hacer clic con el botón derecho sobre ella y seleccionar 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.	Sitúese en la carpeta "%SYSTEMROOT%\Security\Templates" y seleccione el fichero denominado "CCN-STIC-575 ENS Servidor SQL Server 2016 categoria media.inf", seguidamente 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?". 

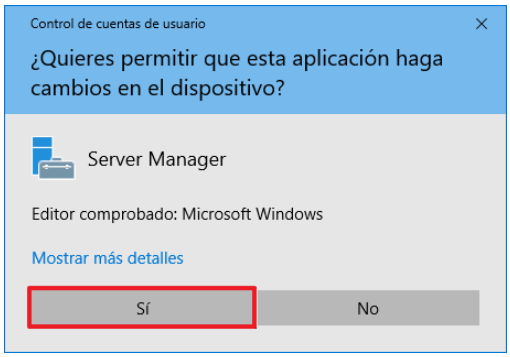
Paso	Descripción
30.	Pulse de nuevo "Aceptar" ante el mensaje de advertencia emergente. 
31.	A continuación, pulse el botón "Agregar…".  **Nota:** En caso de no disponer del grupo mostrado, deberá adaptar estos pasos a las necesidades de su organización.
32.	Introduzca como nombre "ENS Servidores Windows 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.

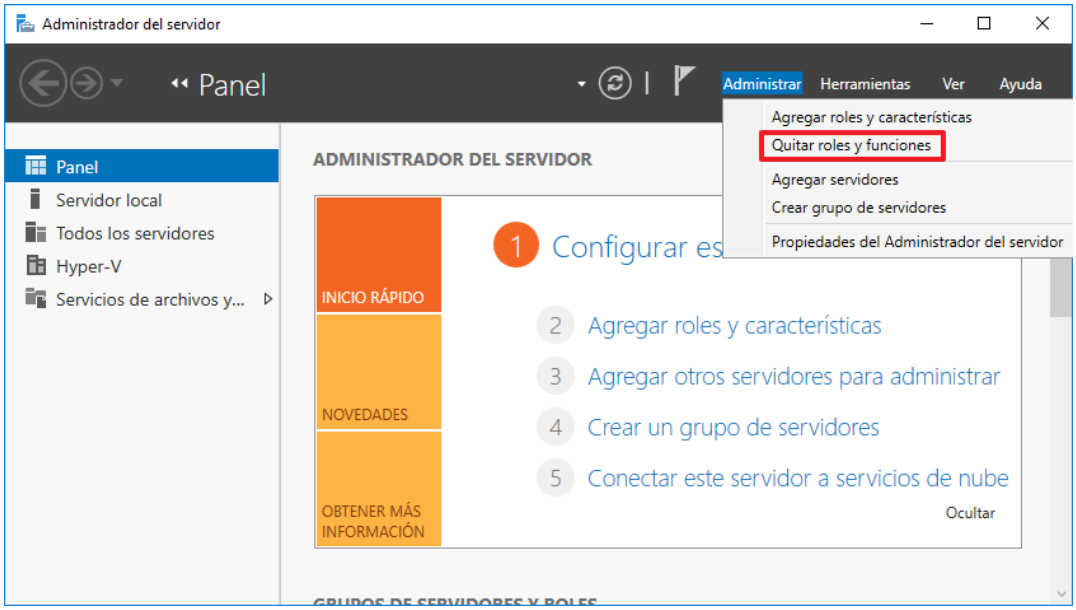
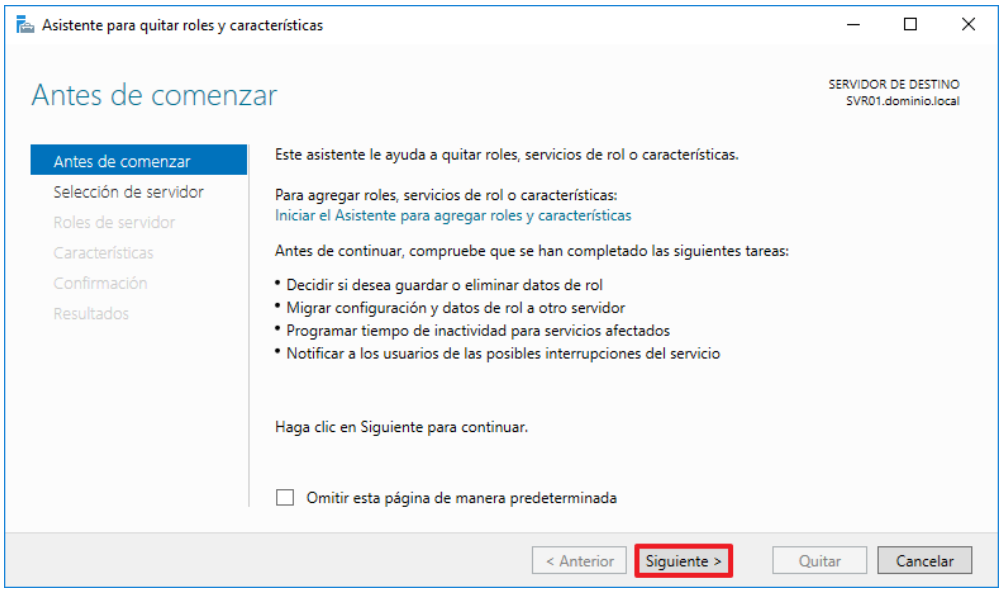
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

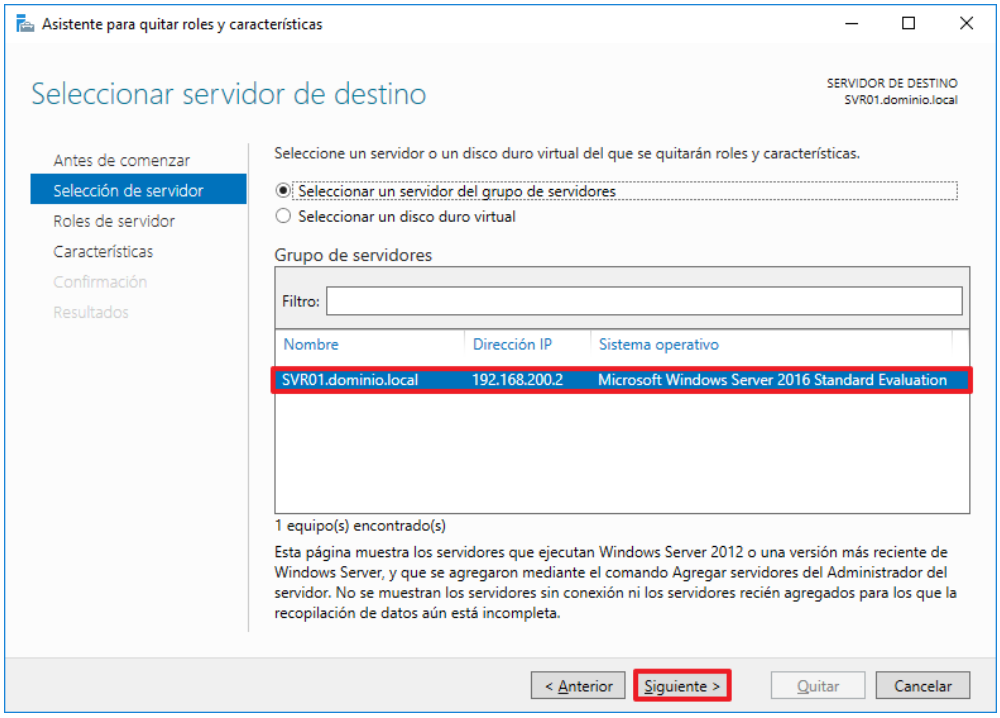
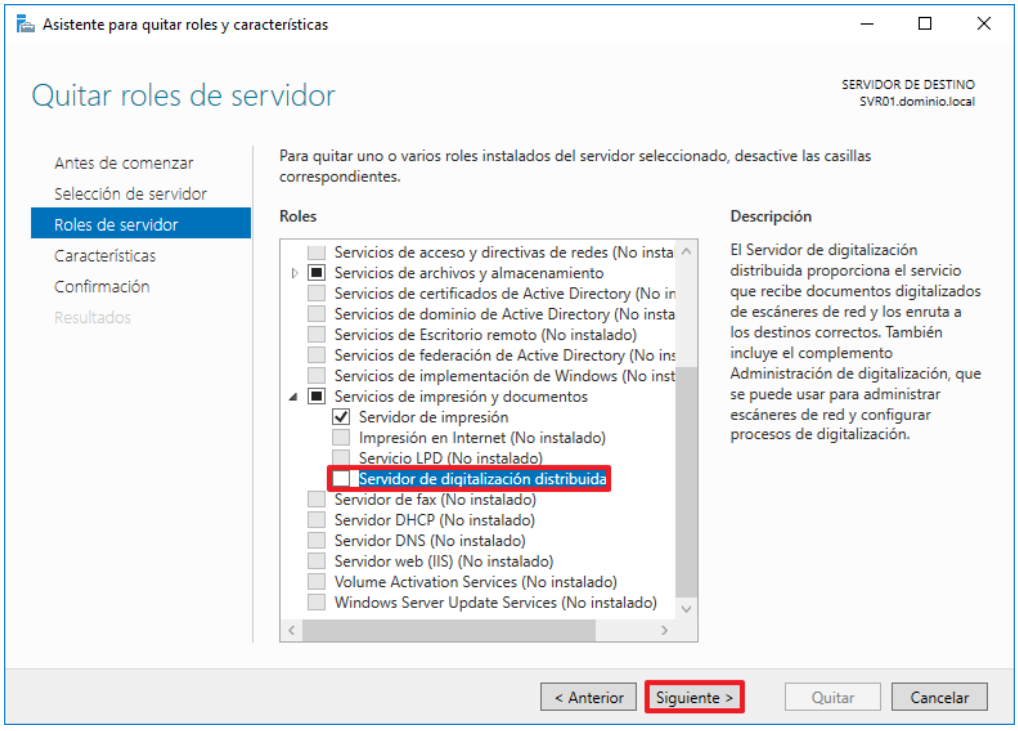
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

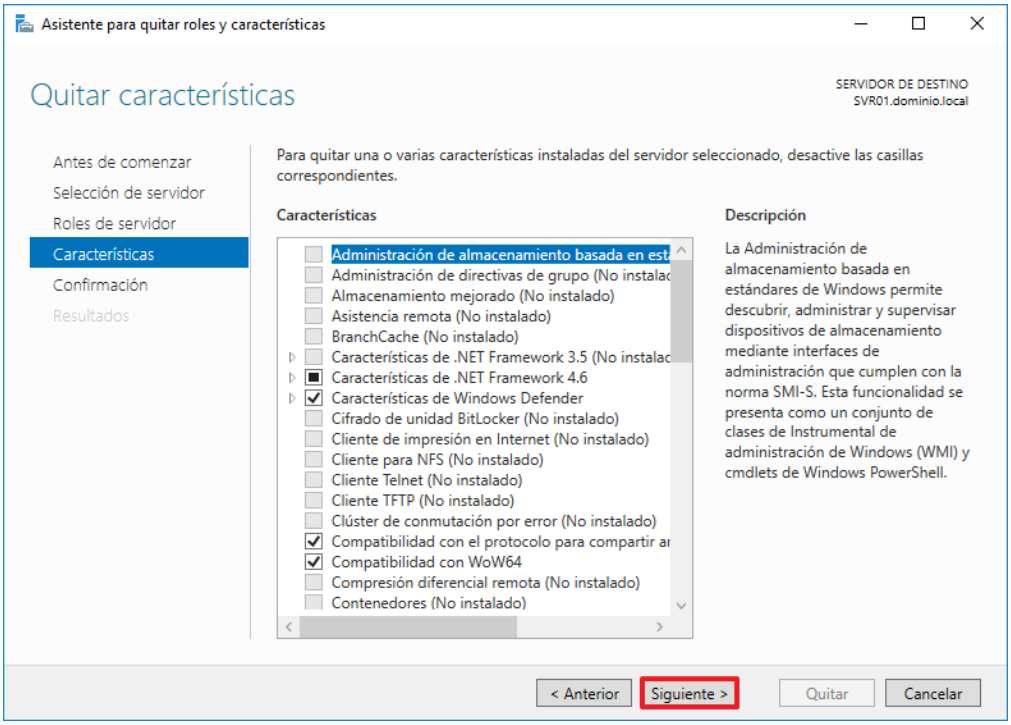
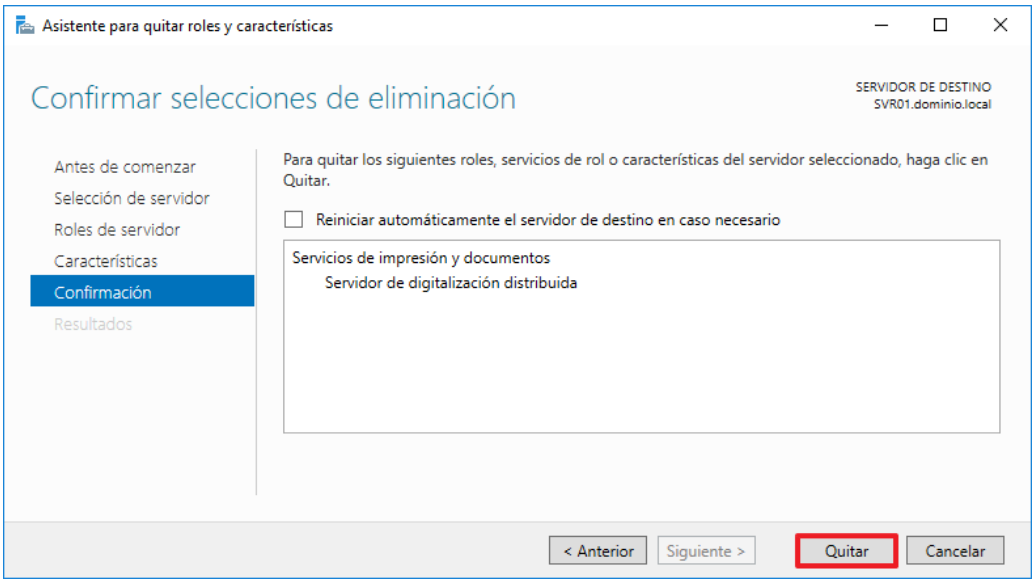
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

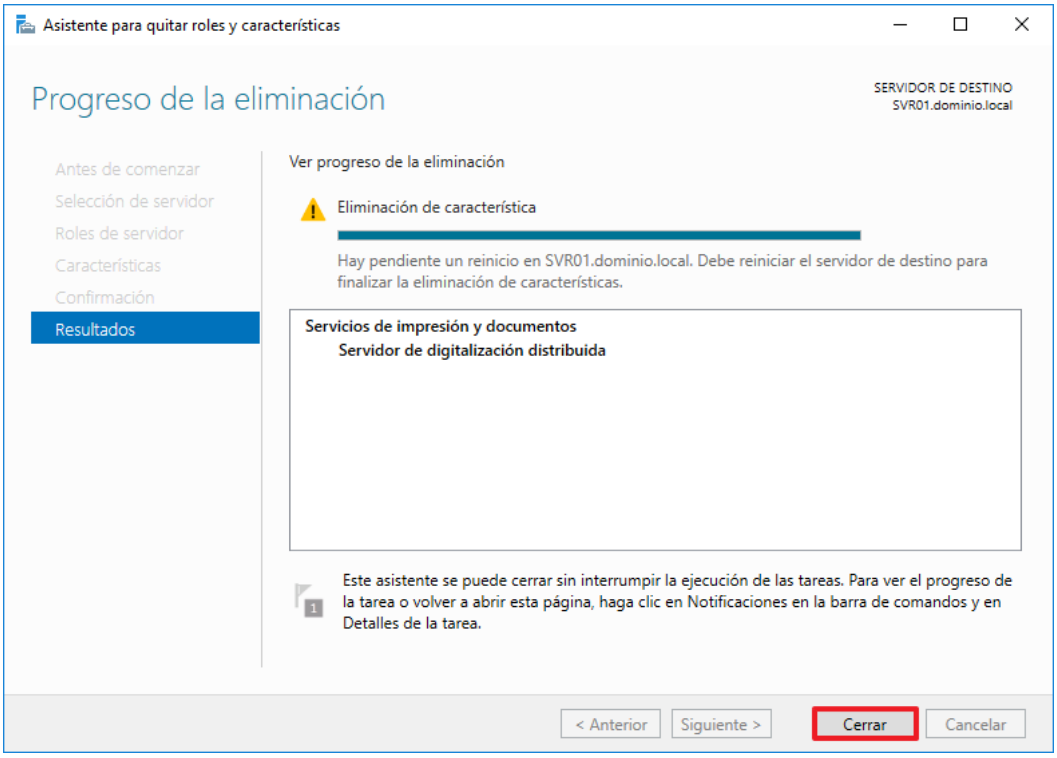
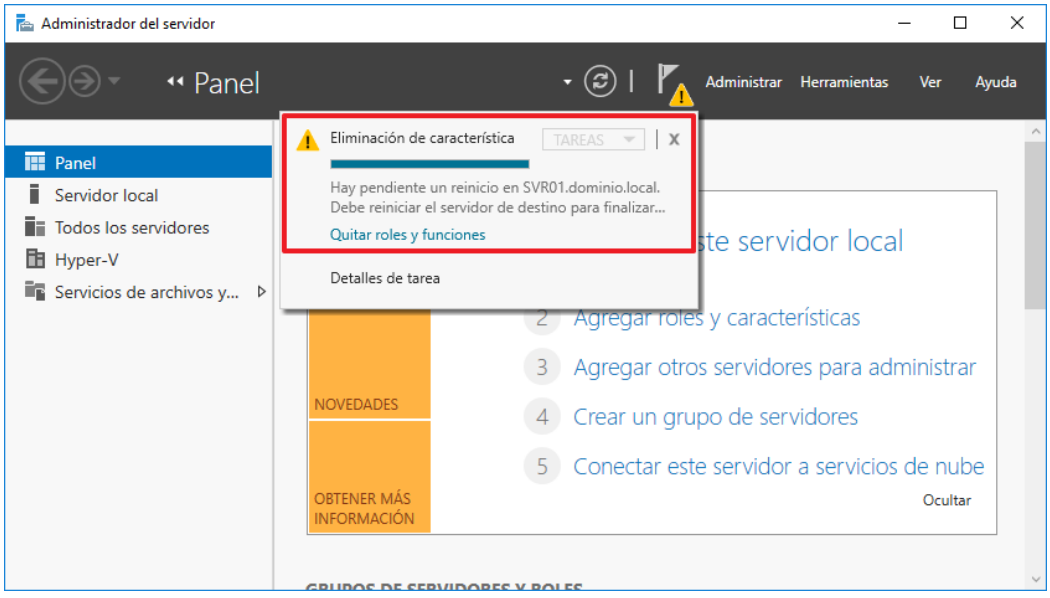
En el procedimiento que se describe a continuación, a modo de ejemplo, desinstala un rol que actualmente no está siendo utilizado.

Paso	Descripción
33.	Inicie sesión en el equipo miembro del dominio donde se va a aplicar seguridad para el Servidor de SQL Server 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. APLICACIÓN DE ESTÁNDARES INTERNACIONALES DE SEGURIDAD

Para que la instalación de SQL Server 2016 cumpla con los estándares internacionales de seguridad, se deben realizar una serie de configuraciones adicionales en el servidor, estas son:

a) Habilitar compatibilidad con dichos estándares de seguridad.

b) Instalar desencadenadores de inicio de sesión.

c) Establecer el proceso de rastreo.

Este procedimiento creará una serie de objetos en la base de datos (tablas, vistas, funciones, triggers y procedimientos almacenados) y un proceso de rastreo que incluye todos los eventos necesarios, junto a la garantía de que este proceso se inicia cada vez que se inicia el servidor. Los objetos creados son los siguientes:

Objeto	Nombre	Descripción
Tabla	denied_logins_A54E382458CA11DB8373B622A1EF5492	Esta tabla contiene los intervalos semanales en la que los inicios de sesión no están autorizados a conectarse a SQL Server. Esta tabla no debe modificarse directamente.
Tabla	maximum_number_of_connections_per_login_A54E382458CA11DB8373B622A1EF5492	Esta tabla contiene el número máximo de conexiones por sesión. Esta tabla no debe modificarse directamente.
Vista	denied_logins	Esta vista vuelca el contenido de la tabla con los intervalos semanales en formato legible por los humanos.
Función	fn_is_original_login_denied_A54E382458CA11DB8373B622A1EF5492	Esta función comprueba si se permite el inicio de sesión original (la que creó la sesión) para iniciar sesión en este momento. El permiso EXECUTE para esta función se concede a todos los usuarios.
Trigger	trig_deny_access_A54E382458CA11DB8373B622A1EF5492	Este trigger se ejecuta en cada intento de inicio de sesión. Comprueba si el login tiene permitido iniciar sesión en ese momento (basado en la hora del día y el día de la semana) y si no se rechaza la conexión lanzando una excepción.
Trigger	trig_max_connections_A54E382458CA11DB8373B622A1EF5492	Este trigger se ejecuta en cada intento de inicio de sesión. Comprueba si el login tiene permitido iniciar sesión en ese momento (basado en el número máximo de sesiones concurrentes por usuario) y si no se rechaza la conexión lanzando una excepción.
Procedimiento almacenado	sp_deny_logon_internal_A54E382458CA11DB8373B622A1EF5492	Procedimiento interno que no debe ejecutarse directamente.
Procedimiento almacenado	sp_deny_logon	Este procedimiento almacenado permite al administrador negar el establecimiento de sesión a un cierto inicio de sesión basado en el día de la semana y la hora del día.

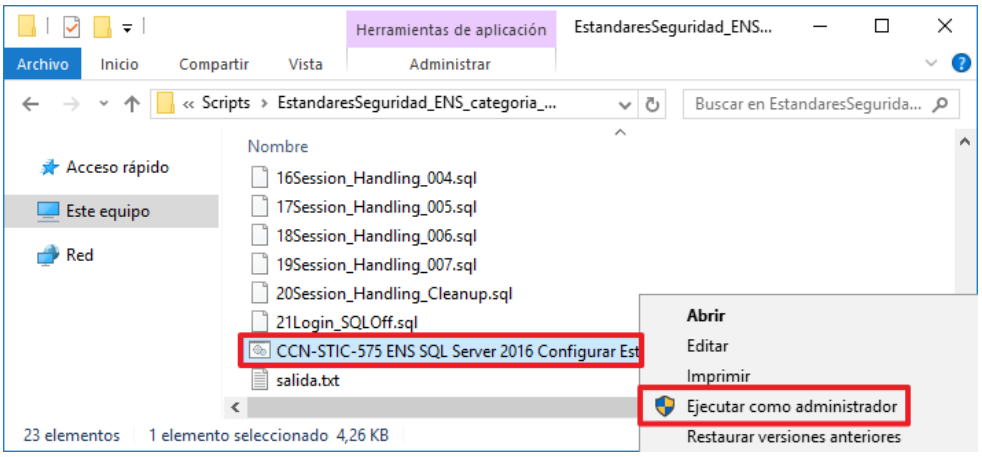
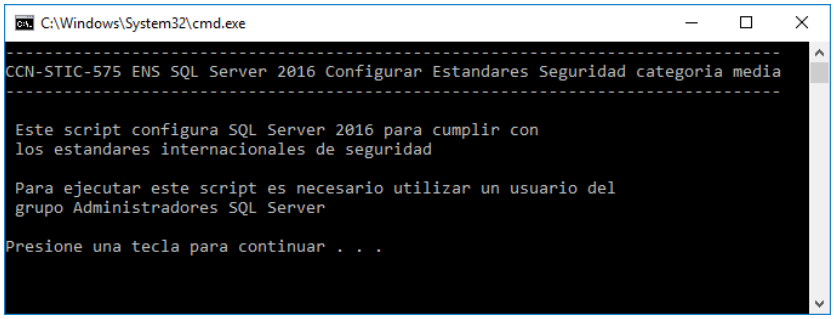
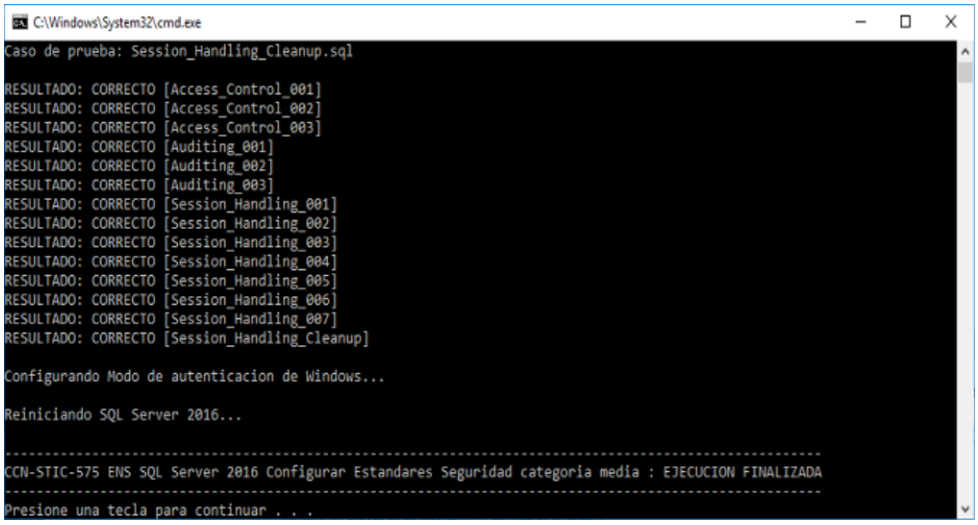
Objeto	Nombre	Descripción
Procedimiento almacenado	sp_revoke_logon_denies	Este procedimiento almacenado permite a un administrador revocar todas las denegaciones de un cierto inicio de sesión.
Procedimiento almacenado	sp_set_maximum_number_of_ connections_per_login	Este procedimiento almacenado permite a un administrador establecer el máximo número de conexiones concurrentes permitidas por inicio de sesión.
Procedimiento almacenado	sp_remove_maximum_number_of_ connections_limit	Este procedimiento almacenado permite a un administrador eliminar la configuración del máximo número de conexiones concurrentes permitidas por inicio de sesión. Tras la ejecución de este procedimiento almacenado, SQL Server dejará de hacer cumplir cualquier limitación en el número de sesiones concurrentes por inicio de sesión.
Procedimiento almacenado	sp_trace_setcategory	Este procedimiento almacenado permite a un administrador habilitar o deshabilitar una columna de datos específica para todos los eventos en una categoría de traza determinada.
Procedimiento almacenado	sp_trace_setcategory_all	Este procedimiento almacenado permite a un administrador habilitar o deshabilitar todas las columnas de datos válidas para todos los eventos en una categoría de traza determinada.

Como resultado del proceso de rastreo, se generarán una serie de ficheros de traza en la carpeta Log de la carpeta raíz de la instancia SQL Server instalada, donde se registrarán todos los eventos.

Además, durante la ejecución de esta fase se activa la auditoría de inicios de sesión correctos y erróneos.

A continuación, se muestran los pasos necesarios para llevar a cabo esta configuración.

Paso	Descripción
44.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
45.	Localice la carpeta "C:\Scripts\EstandaresSeguridad_ENS_categoria_media" que previamente se ha copiado al equipo. **Nota:** En caso de no disponer de la carpeta "C:\Scripts" deberán copiar los archivos necesarios en la ruta "C:\Scripts" para continuar con la ejecución del paso a paso.

Paso	Descripción
46.	Ejecute el script "CCN-STIC-575 ENS SQL Server 2016 Configurar Estandares Seguridad categoria media.bat" con privilegios de administración. Para ello, pulse con el botón derecho "Ejecutar como administrador". 
47.	El "Control de cuentas de usuarios" le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador de dominio y pulse "Sí".
48.	Pulse una tecla para aplicar los estándares internacionales de seguridad. 
49.	Espere a que finalice el proceso. Puede tardar varios minutos en completarse. Una vez finalizada la configuración, presione una tecla para cerrar la ventana.  **Nota:** Omita cualquier advertencia de error que se encuentre fuera del rango de valores "Resultado".

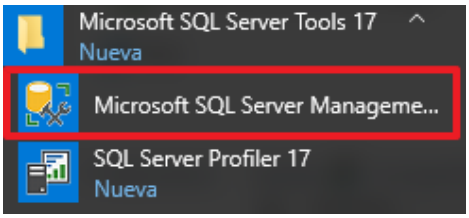
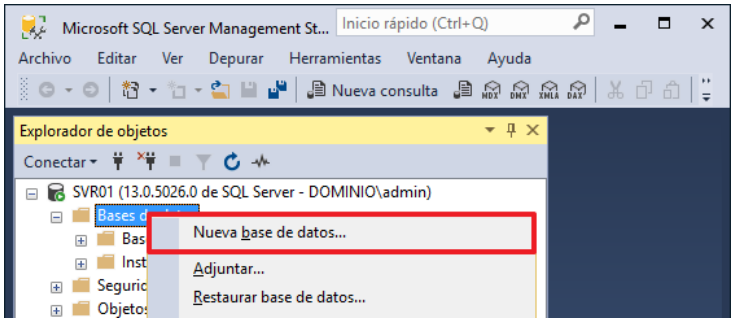
Paso	Descripción
50.	Compruebe que el resultado de todas las pruebas es "CORRECTO". **Nota:** Durante este proceso se activa el modo de autenticación de Windows y SQL para poder llevar a cabo parte de las pruebas. Al finalizar el proceso se vuelve a configurar el Modo de autenticación de Windows.
51.	Pulse una tecla para finalizar la ejecución de la configuración y cerrar la ventana.
52.	Para que el sistema termine de aplicar los cambios deberá reiniciar el servidor donde están aplicando las configuraciones de seguridad.

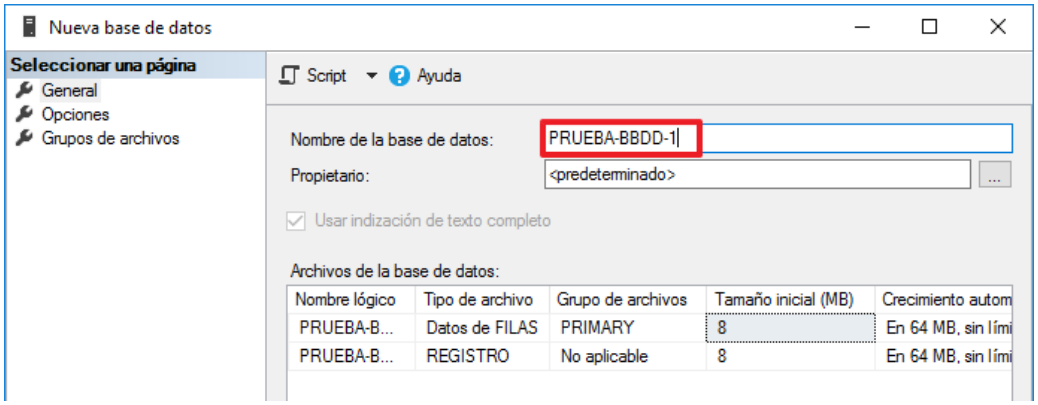
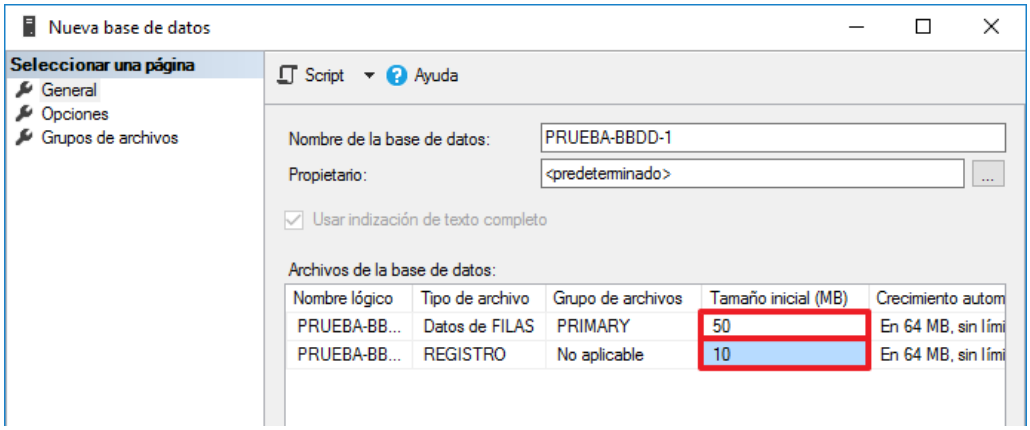
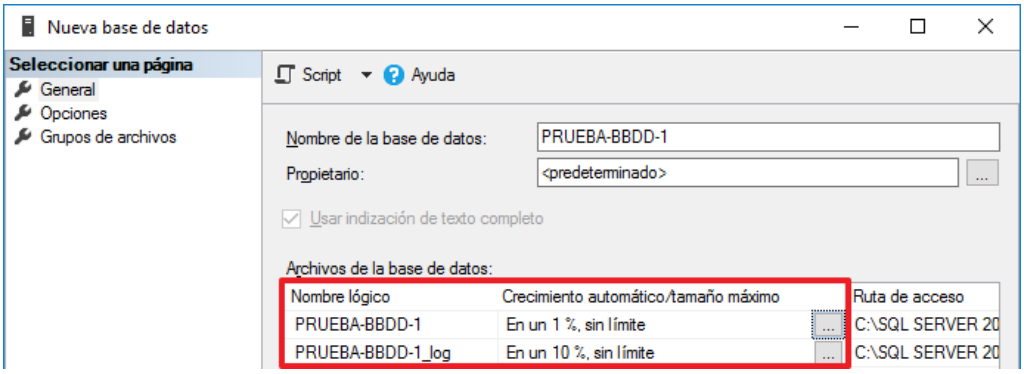
2.3. GESTIÓN DE BASES DE DATOS

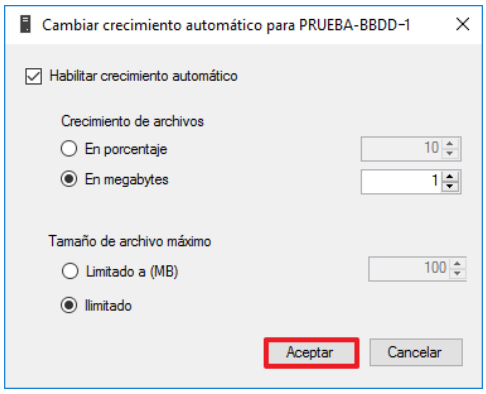
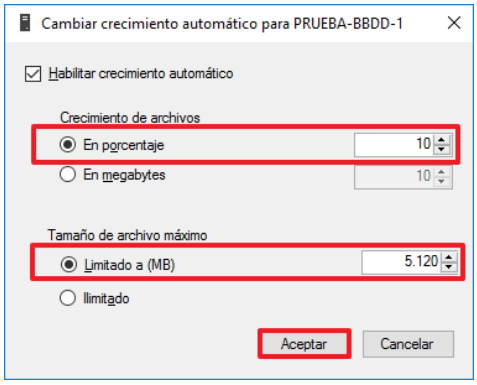
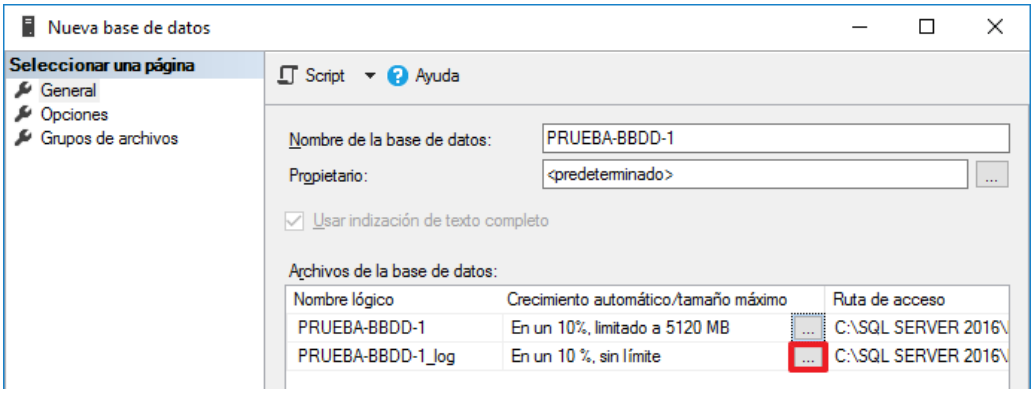
Las bases de datos son el componente sobre el que se apoya SQL Server 2016 para almacenar toda la información que se genera. Este apartado define un ejemplo de cómo gestionar dichas bases de datos.

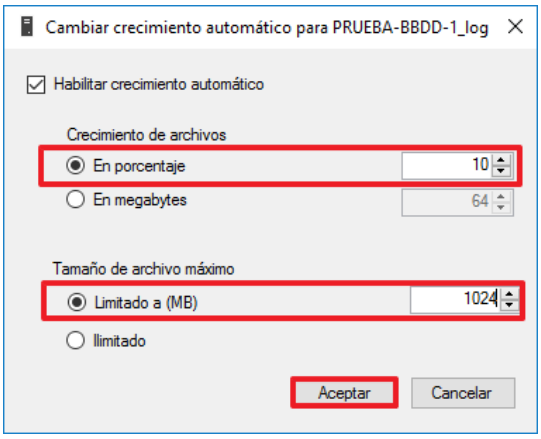
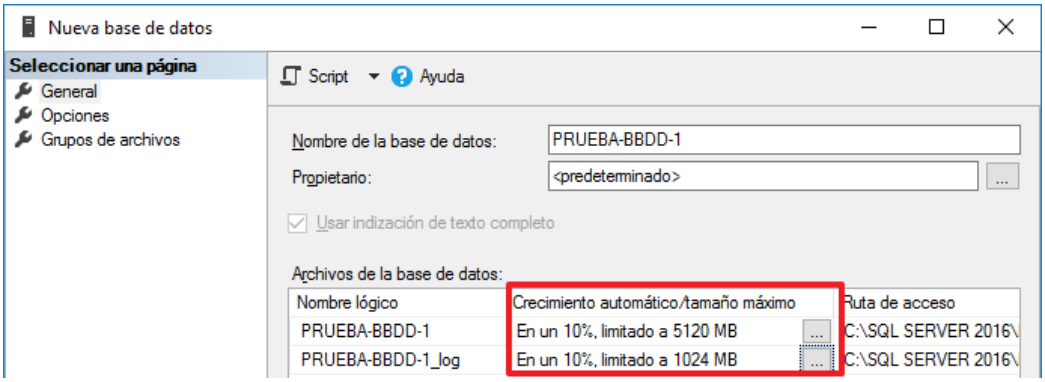
2.3.1. CREACIÓN DE BASES DE DATOS

En esta sección se definen los pasos para crear una nueva base de datos en el servidor SQL.

Paso	Descripción
53.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
54.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
55.	En la ventana de "Conectar con el servidor", es necesario asegurarse que el nombre del servidor es el correcto y pulse "Conectar".
56.	Despliegue el nodo "Bases de datos" y con el botón derecho, seleccione la opción del menú contextual "Nueva base de datos". 

Paso	Descripción
57.	Escriba el nombre de la base de datos que se desea crear.  **Nota:** En este ejemplo se utiliza el nombre "PRUEBA-BBDD-1".
58.	En la zona de archivos de la base de datos, puede especificar el tamaño inicial de la base de datos y el grado de crecimiento automático que se desea aplicar. Por ejemplo, si desea crear una base de datos con 50 MB de tamaño inicial y un fichero de registro de transacciones (log) con 10 MB, entonces establezca los valores 50 y 10 respectivamente. 
59.	En la columna de crecimiento automático, se establece el grado de crecimiento que se desea implementar para ambos ficheros una vez que se haya alcanzado el tamaño inicial establecido. 

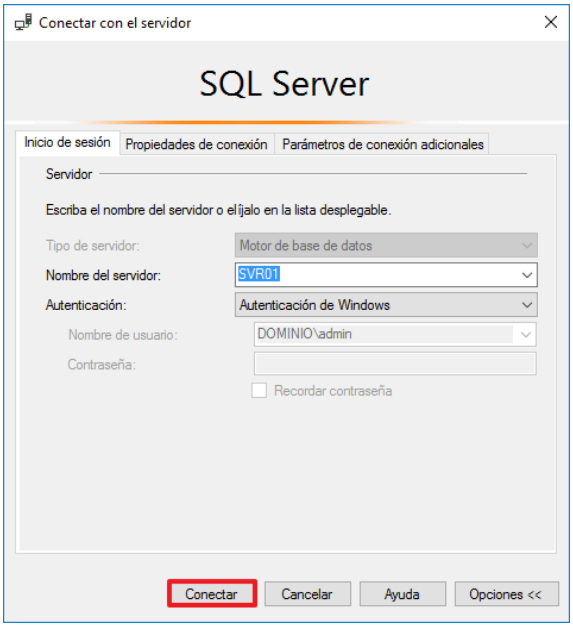
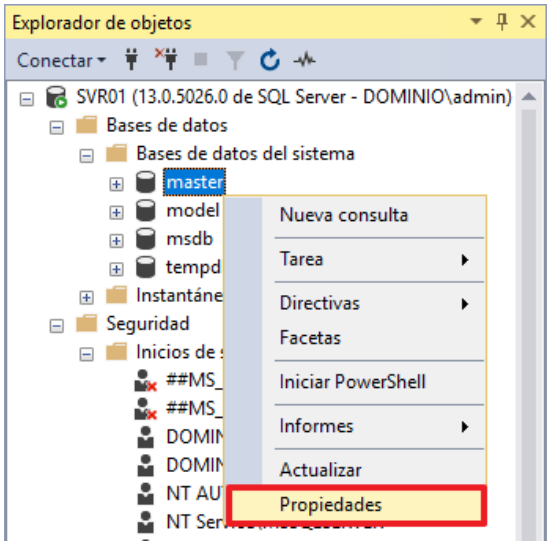
Paso	Descripción
60.	Pulse sobre el primero de los botones "…" para establecer el grado de crecimiento de la base de datos. Pulse "Aceptar" para guardar los cambios.  **Nota:** Puede establecerse el crecimiento en un porcentaje relativo al tamaño de la base de datos o en un valor estático en megabytes (MB). También puede limitarse el crecimiento a un tamaño máximo, para evitar que se pueda consumir todo el espacio del disco físico.
61.	En este ejemplo se va a configurar el crecimiento automático en un porcentaje de 10%, con un límite máximo de 5 GB para la base de datos y 1 GB para el fichero de registro de transacciones.
62.	Seleccione la opción "En porcentaje" y escriba 10. A continuación seleccione la "Limitar el crecimiento de los archivos (MB)" y escriba 5120. Pulse sobre "Aceptar". 
63.	Pulse sobre el segundo de los botones "…" para establecer el grado de crecimiento del fichero de registro de transacciones de la base de datos. 

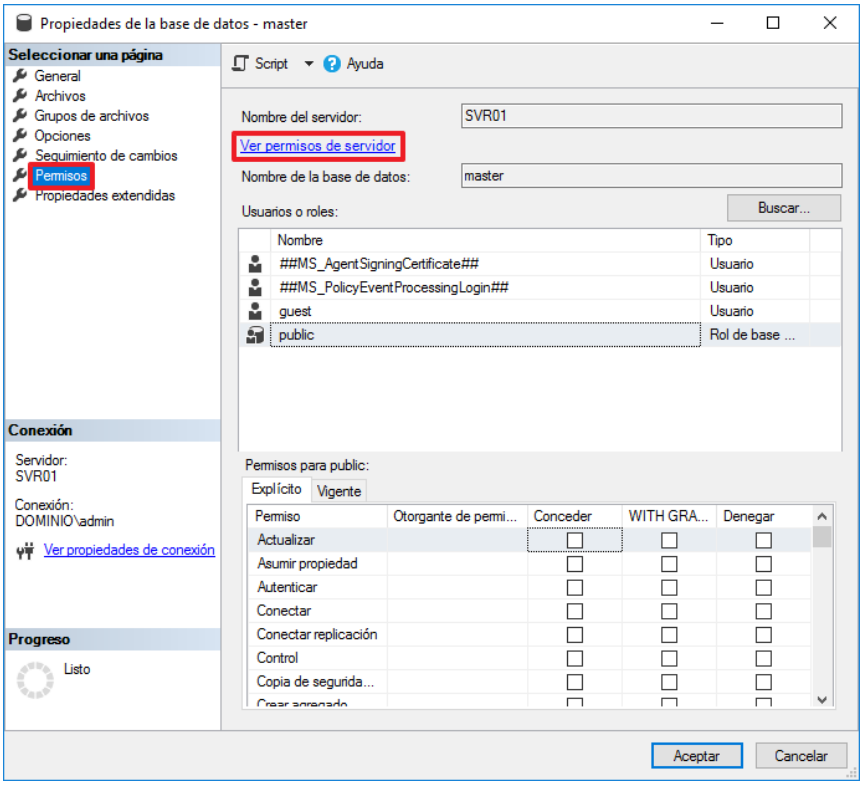
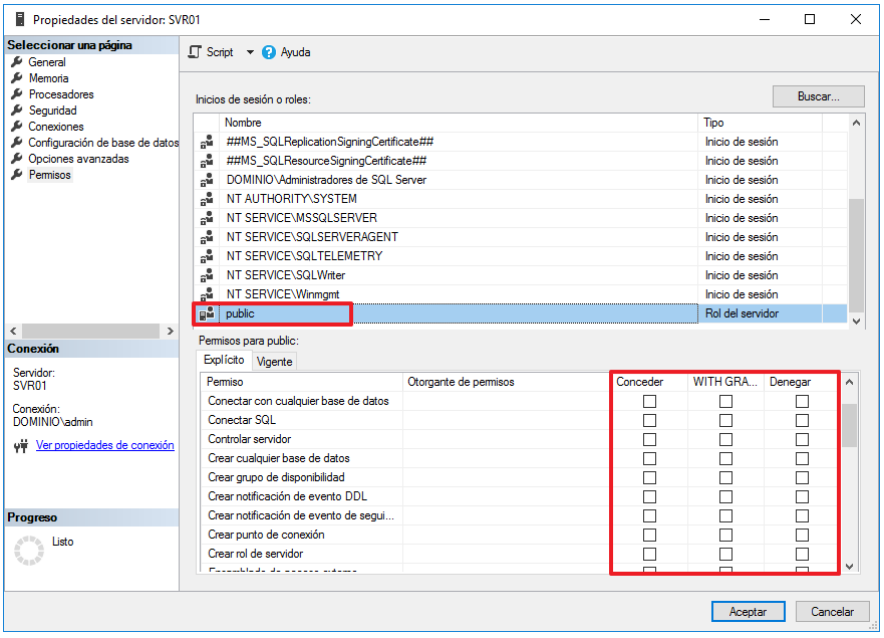
Paso	Descripción
64.	Debe seleccionarse la opción "En porcentaje" y escriba 10. A continuación seleccione la opción "Limitado a (MB)" y escriba 1024. Pulse sobre el botón "Aceptar". 
65.	Compruebe que los valores introducidos son correctos. 

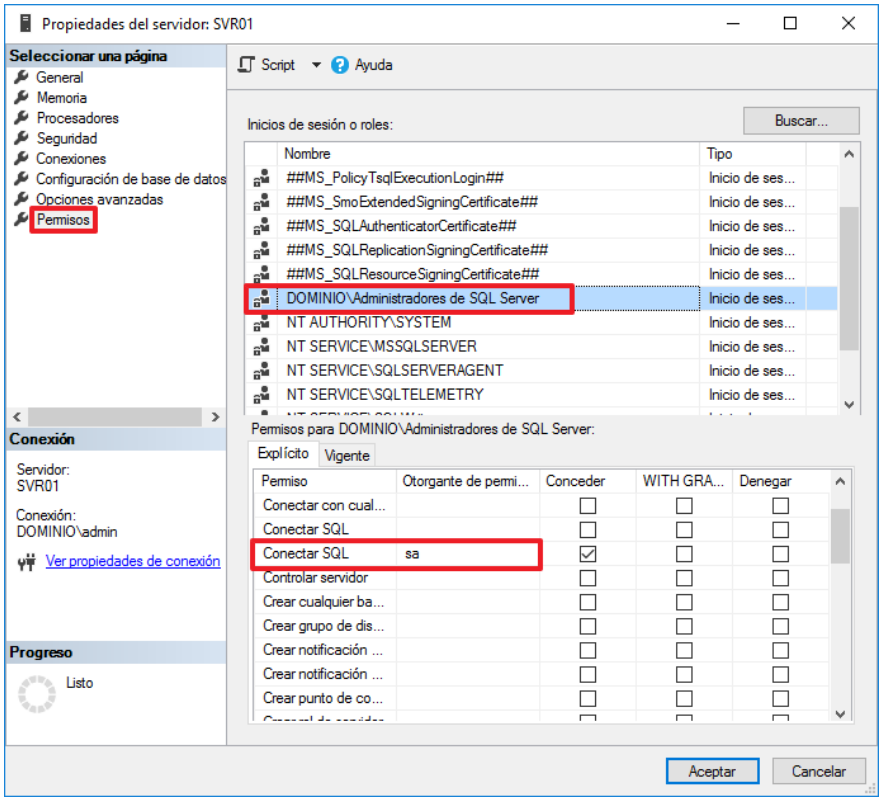
2.3.2. MODIFICACIÓN DE BASES DE DATOS

En esta sección se definen los pasos para modificar parámetros de seguridad de una base de datos en el servidor SQL.

Paso	Descripción
66.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
67.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**.

Paso	Descripción
68.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar". 
69.	En la consola "SQL Server Management Studio", seleccione la carpeta "Bases de datos" y diríjase a aquella base de datos que quiera modificar dentro de "Bases de datos del sistema".  **Nota:** En este ejemplo, se modificará la base de datos "master".

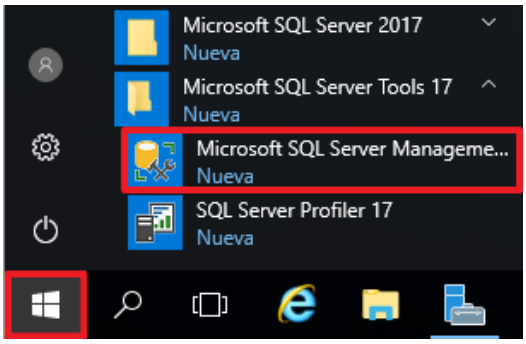
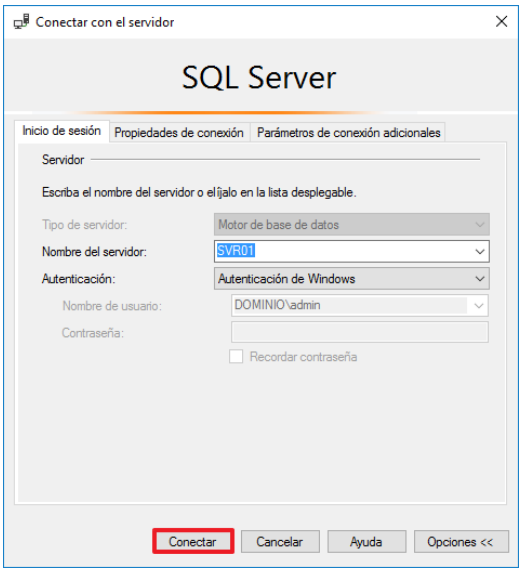
Paso	Descripción
70.	Seleccione la pestaña "Permisos" del panel izquierdo y finalmente pulse en la opción "Ver permisos del servidor". 
71.	En esta pantalla puede cambiar los permisos de cada inicio de sesión y/o rol del servidor. marcando los distintos inicios de sesión en el panel superior se muestran los permisos de éste. 

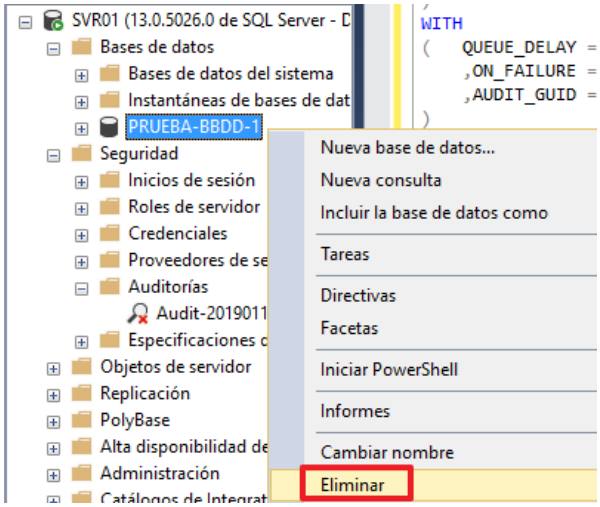
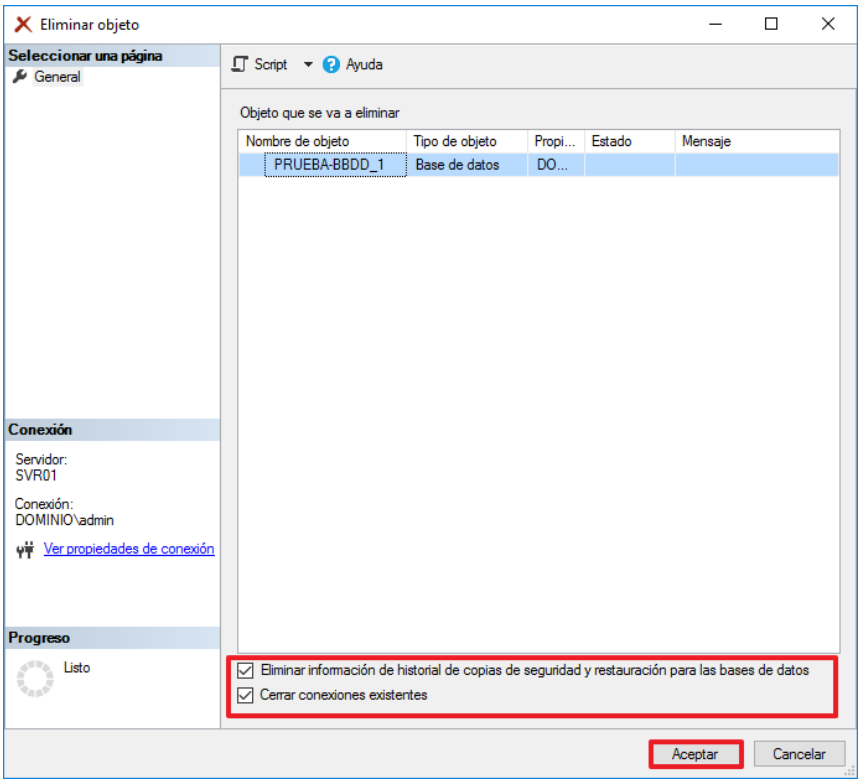
Paso	Descripción
72.	Es necesario asegurarse que después de haber dado de alta todos los inicios de sesión necesarios de su organicación tan sólo un inicio de sesión o rol puede cambiar los permisos del resto de usuarios tal y como se ve en la siguiente pantalla.  **Nota:** Para más información sobre los servicios de servidores asociados a las cuentas de SQL Server puede consultar la página https://docs.microsoft.com/es-es/sql/database-engine/configure-windows/configure-windows-service-accounts-and-permissions?view=sql-server-2016.

2.3.3. ELIMINACIÓN DE BASES DE DATOS

En esta sección se definen los pasos para eliminar una base de datos en el servidor SQL.

Paso	Descripción
73.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.

Paso	Descripción
74.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
75.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar". 

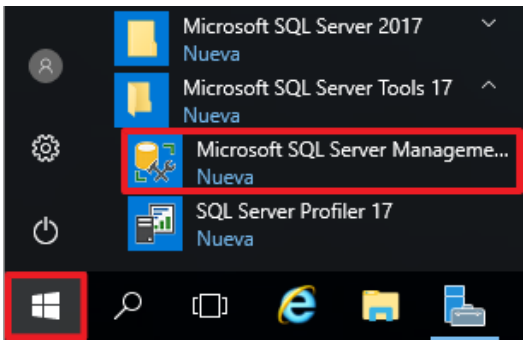
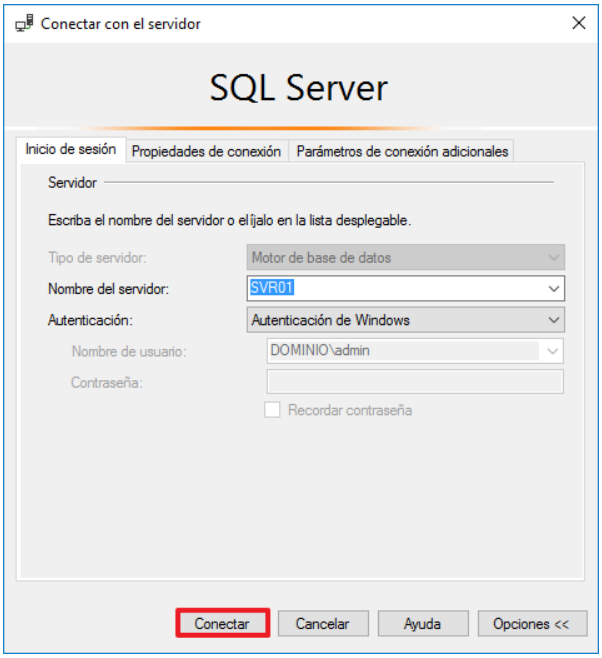
Paso	Descripción
76.	Sitúese en el nodo del árbol "Bases de datos" y seleccione la base de datos que quiera eliminar. Haga clic derecho sobre ella y pulse "Eliminar".  **Nota:** En este ejemplo se procede a eliminar la base de datos llamada "PRUEBA-BBDD-1".
77.	En la siguiente pantalla, marque las opciones "Eliminar información de historial de copias de seguridad y restauración para las bases de datos" y "Cerrar conexiones existentes", finalmente pulse "Aceptar" para eliminar la base de datos. 

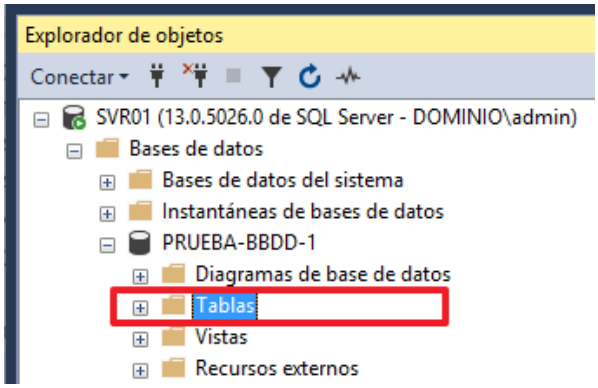
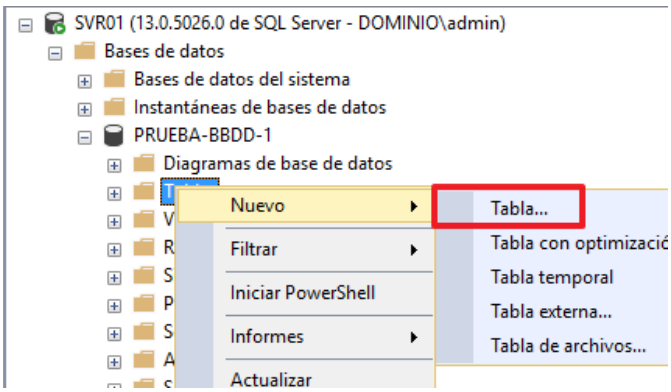
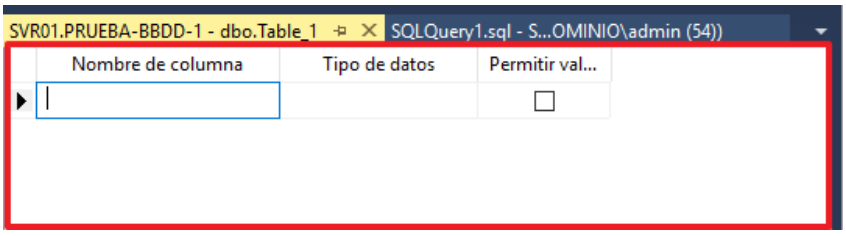
2.4. GESTIÓN DE TABLAS

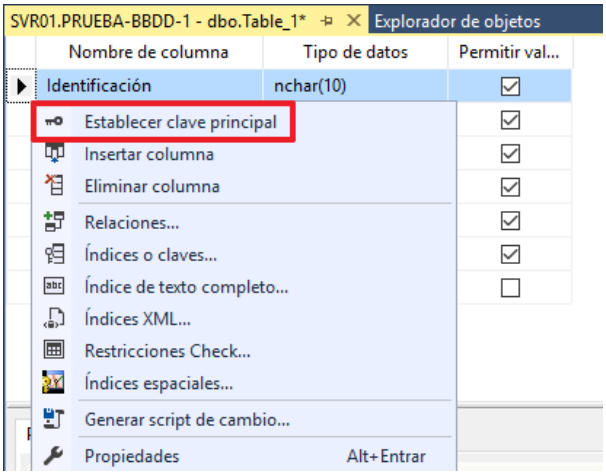
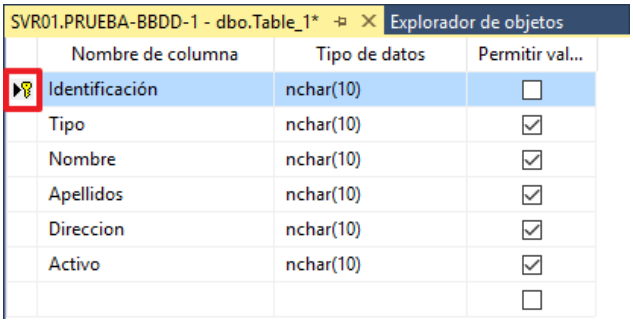
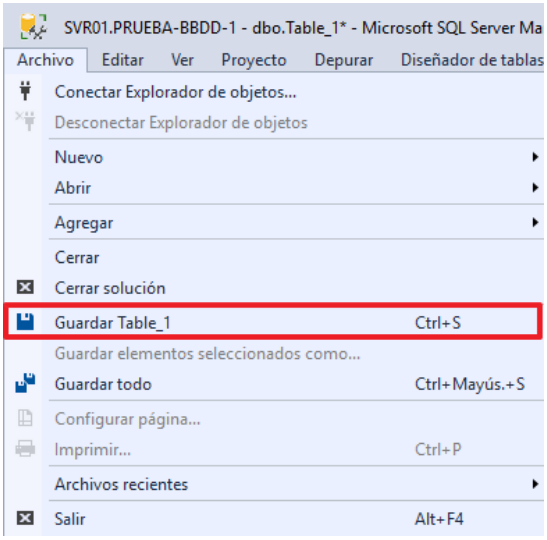
La gestión de tablas dentro de SQL Server 2016 constituye una importante tarea de administración debido a que permite establecer o modificar configuraciones que afectan a la funcionalidad del servicio de base de datos.

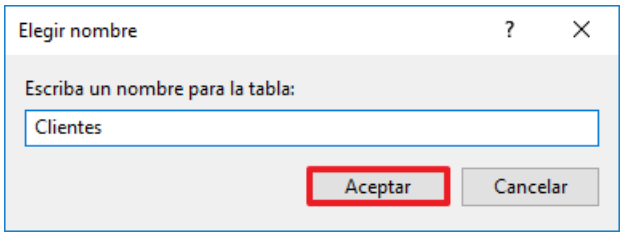
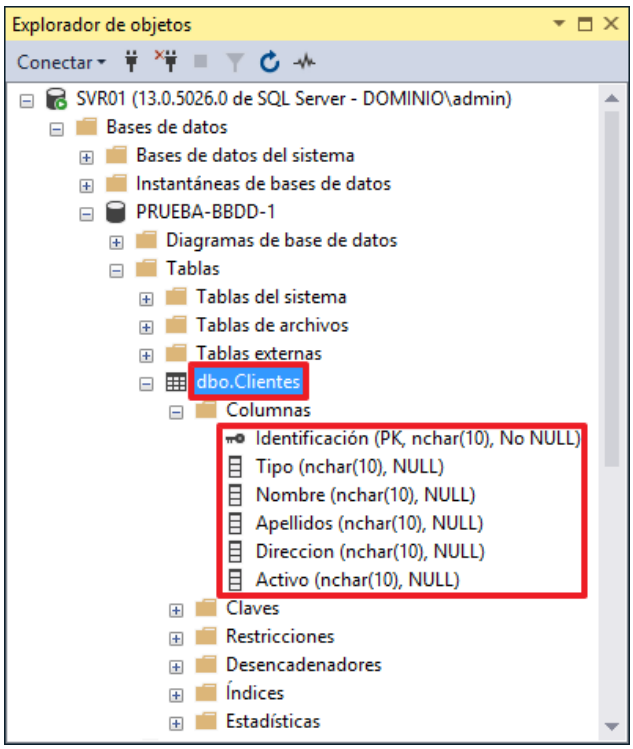
2.4.1. CREACIÓN DE TABLAS

En este apartado se definen los pasos para crear una nueva base de datos en el servidor SQL.

Paso	Descripción
78.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
79.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".** 
80.	En la ventana de "Conectar con el servidor", asegúrese de que el nombre del servidor es el correcto y pulse "Conectar". 

Paso	Descripción
81.	En la consola "SQL Server Management Studio", sitúese en la base de datos donde desee crear una nueva tabla y diríjase a la carpeta "Tablas". la carpeta "Tablas" de la base de datos "PRUEBA-BBDD-1" creada anteriormente, tal y como se observa en la imagen.  **Nota:** En este ejemplo, se creará una tabla dentro de la base de datos "PRUEBA-BBDD-1".
82.	Con el botón derecho sobre "Tablas", seleccione la opción del menú contextual **"Nuevo → Tabla…".** 
83.	En el área "Nombre de columna", establezca un nombre a cada una de las columnas que va a tener la nueva tabla, así como el tipo de dato correspondiente.  **Nota:** Se recomienda no incluir caracteres especiales en los nombres de las columnas, tales como tildes, signos de exclamación, interrogación o cedillas.

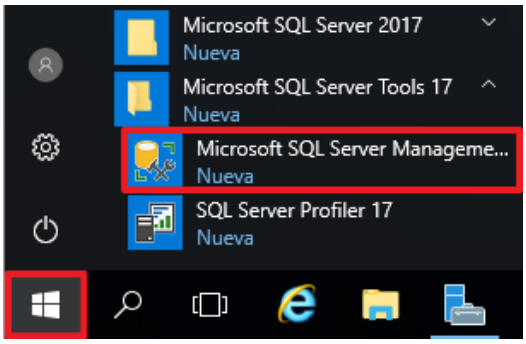
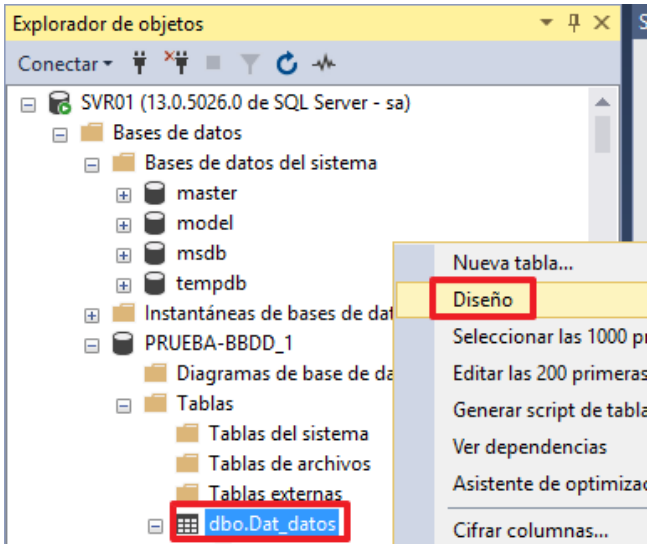
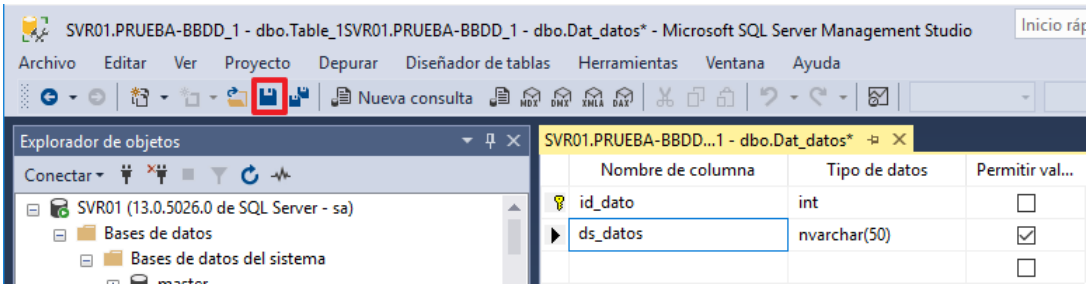
Paso	Descripción
84.	Cuando haya finalizado de introducir las diferentes columnas, será necesario establecer una clave principal dentro de la nueva tabla. Para ello, seleccione aquella columna que desea establecer como llave primaria y pulsando con el botón derecho sobre ella, seleccione la opción del menú contextual "Establecer clave primaria".  **Nota:** En este ejemplo, se utiliza la columna "Identificación".
85.	Asegúrese que aparece una llave sobre la columna que ha establecido como clave primaria como se muestra en la siguiente imagen. 
86.	Para guardar los cambios realizados, pulse sobre la opción del menú contextual **"Archivo → Guardar Table_1".** 

Paso	Descripción
87.	Establezca un nombre para la nueva tabla acorde a las necesidades de su organización y pulse sobre el botón "Aceptar".  **Nota:** En este ejemplo, se utiliza el nombre "Clientes".
88.	Ahora, en el Explorador de objetos, acceda a la nueva tabla para obervar las columnas creadas en pasos anteriores. 

2.4.2. MODIFICACIÓN DE TABLAS

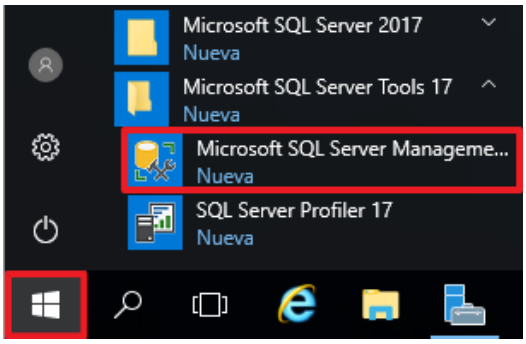
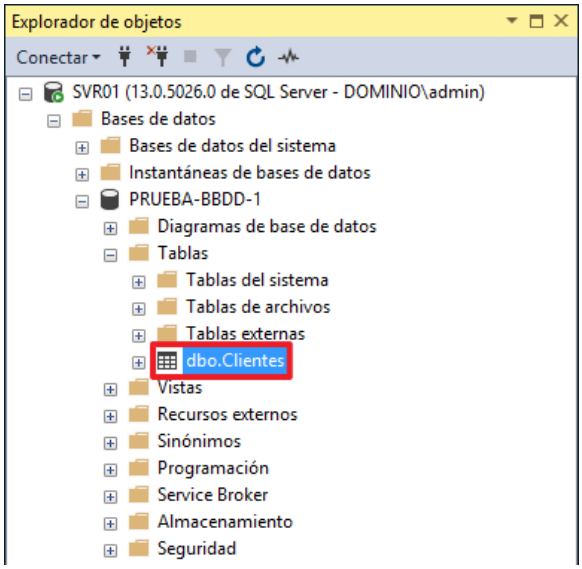
En este apartado se define como modificar una tabla desde SQL Server Management Studio.

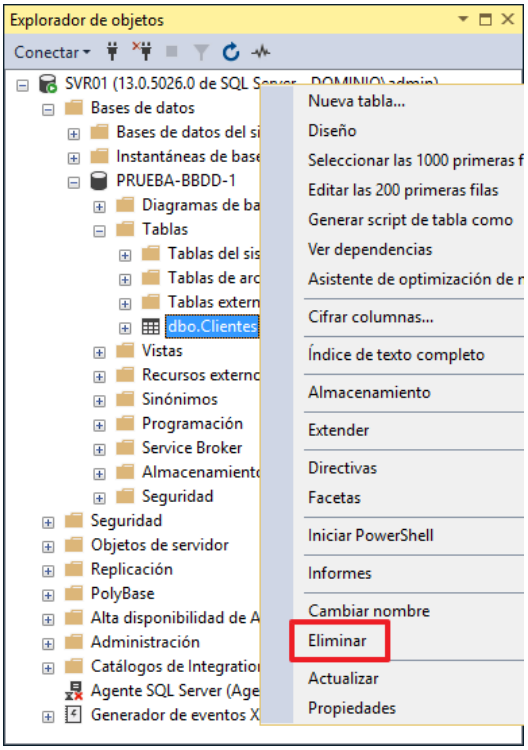
Paso	Descripción
89.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.

Paso	Descripción
90.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
91.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".
92.	En la consola "SQL Server Management Studio" localice la tabla que desea modificar, y pulsando con el botón derecho sobre ella, seleccione la opción del menú contextual "Diseño". 
93.	Ahora, podrá realizar los cambios que considere oportunos para su organización. Para guardar los cambios, pulse el botón "guardar". 

2.4.3. ELIMINACIÓN DE TABLAS

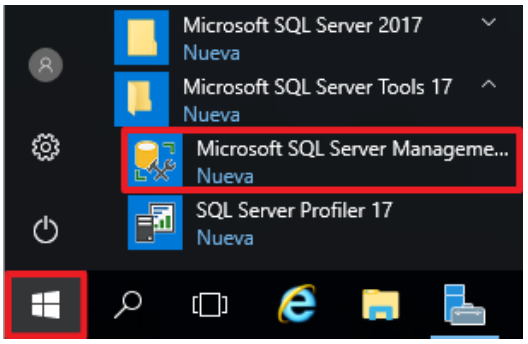
En este apartado se define como eliminar una tabla desde SQL Server Management Studio.

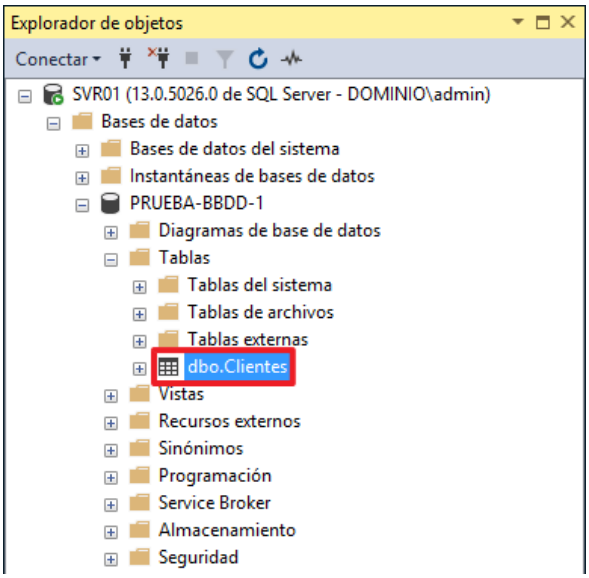
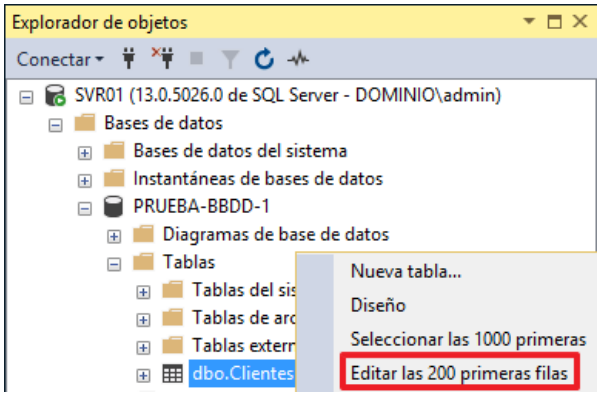
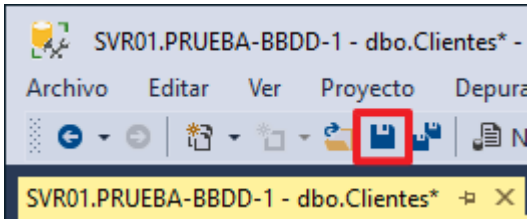
Paso	Descripción
94.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
95.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".** 
96.	En la ventana de "Conectar con el servidor", asegúrese de que el nombre del servidor es el correcto y pulse "Conectar".
97.	Dentro del Explorador de objetos, expanda el árbol "Bases de datos" hasta llegar a la tabla que desea eliminar.  **Nota:** En este ejemplo, se utiliza la tabla "dbo.Clientes".

Paso	Descripción
98.	Una vez seleccionada la tabla, haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Eliminar". 

2.4.4. INSERCIÓN DE DATOS

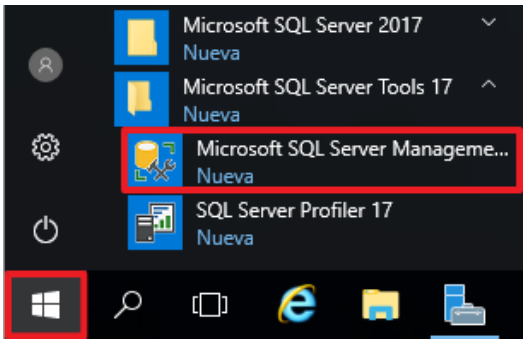
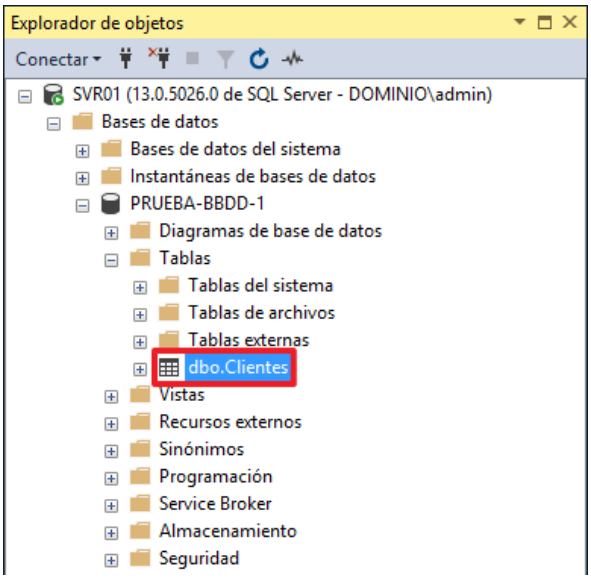
En este apartado se define como insertar datos desde SQL Server Management Studio.

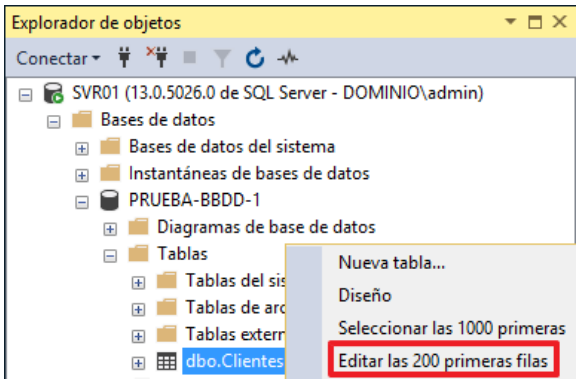
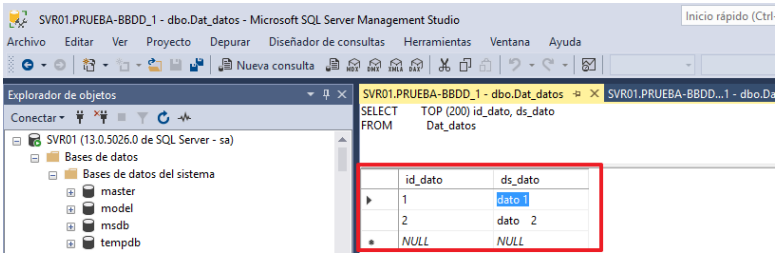
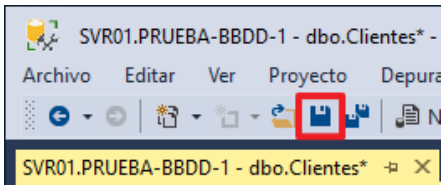
Paso	Descripción
99.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
100.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
101.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".

Paso	Descripción
102.	Dentro del Explorador de objetos, expanda el árbol "Bases de datos" hasta llegar a la tabla que desea insertar datos.  **Nota:** En este ejemplo, se utiliza la tabla "dbo.Clientes".
103.	Una vez seleccionada la tabla, haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Editar las 200 primeras filas" para insertar los datos en la tabla seleccionada. 
104.	Una vez finalizada la inserción de datos, pulse el botón "Guardar" para salvaguardar los datos introducidos. 

2.4.5. MODIFICACIÓN DE DATOS

En este apartado se define como modificar datos desde SQL Server Management Studio.

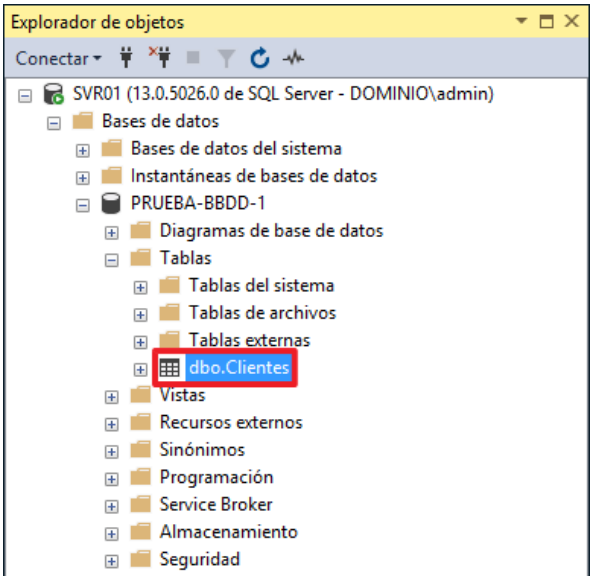
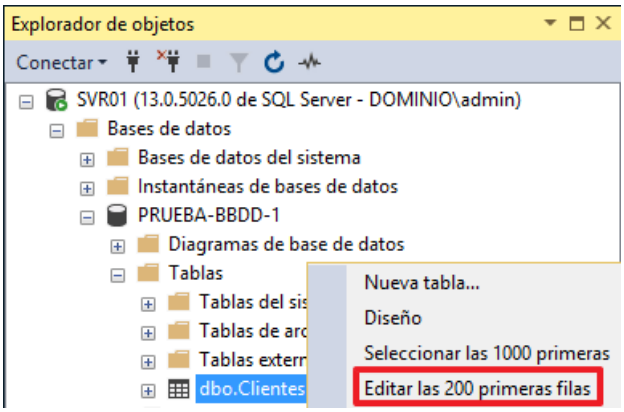
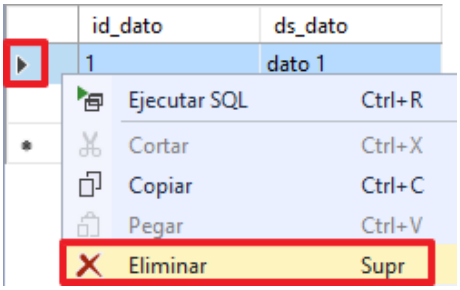
Paso	Descripción
105.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
106.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
107.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".
108.	Dentro del Explorador de objetos, expanda el árbol "Bases de datos" hasta llegar a la tabla que desea insertar datos.  **Nota:** En este ejemplo, se utiliza la tabla "dbo.Clientes".

Paso	Descripción
109.	Una vez seleccionada la tabla, haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Editar las 200 primeras filas". 
110.	En la siguiente ventana, puede insertar y modificar los datos acorde a las necesidades de su organización. 
111.	Una vez finalizada la modificación de datos, pulse el botón "Guardar" para salvaguardar los datos modificados. 

2.4.6. ELIMINACIÓN DE DATOS

En este apartado se define como eliminar datos desde SQL Server Management Studio.

Paso	Descripción
112.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
113.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**.
114.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".

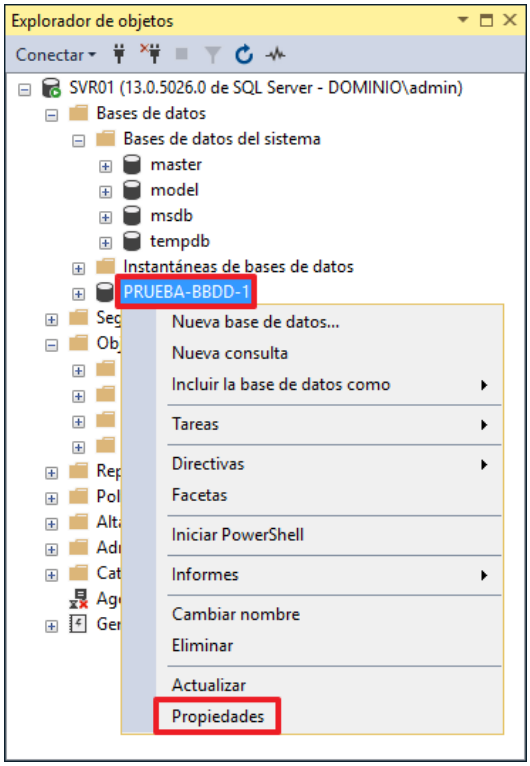
Paso	Descripción
115.	Dentro del Explorador de objetos, expanda el árbol "Bases de datos" hasta llegar a la tabla que en la que desea eliminar un dato.  **Nota:** En este ejemplo, se utiliza la tabla "dbo.Clientes".
116.	Una vez seleccionada la tabla, haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Editar las 200 primeras filas" para insertar los datos en la tabla seleccionada. 
117.	Haga clic derecho sobre fila que desea eliminar y pinche sobre la opción del menú contextual "Eliminar" para borrar el registro seleccionado. 

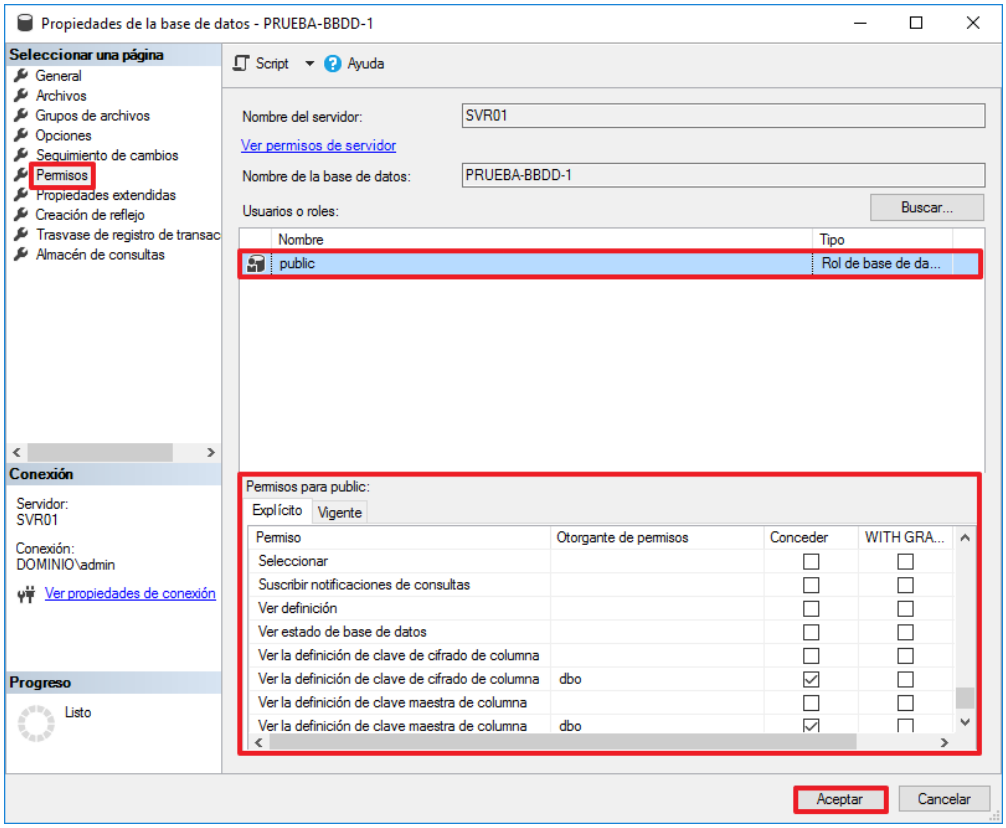
2.5. ASIGNACIÓN DE PERMISOS SOBRE SQL

Los permisos de acceso sobre los diferentes datos dentro de SQL Server 2016 debe quedar limitado a los usuarios legitimados para ello. Por lo tanto, será necesario establecer los permisos necesarios para limitar dicho acceso.

2.5.1. PERMISOS EN BASES DE DATOS

En este procedimiento se describen los procesos para alterar los permisos de diferentes objetos de la base de datos.

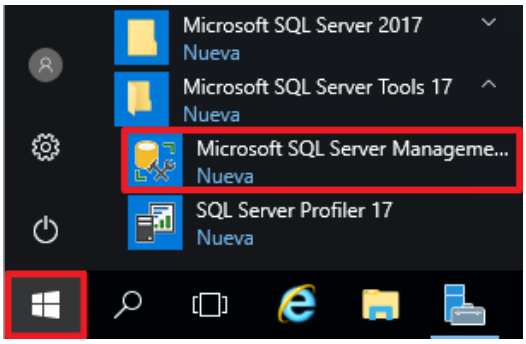
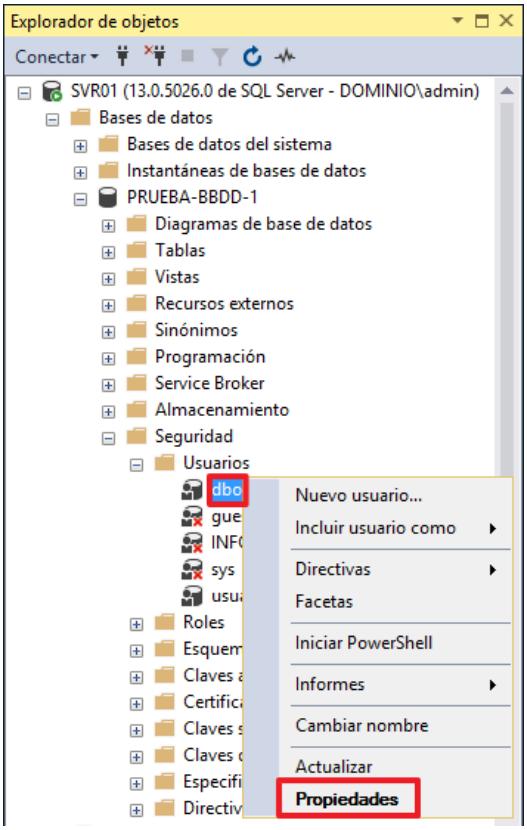
Paso	Descripción
118.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
119.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".**
120.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".
121.	Una vez seleccionada la tabla, haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Propiedades".  **Nota:** En este ejemplo, se utiliza la base de datos "PRUEBA-BBDD-1".

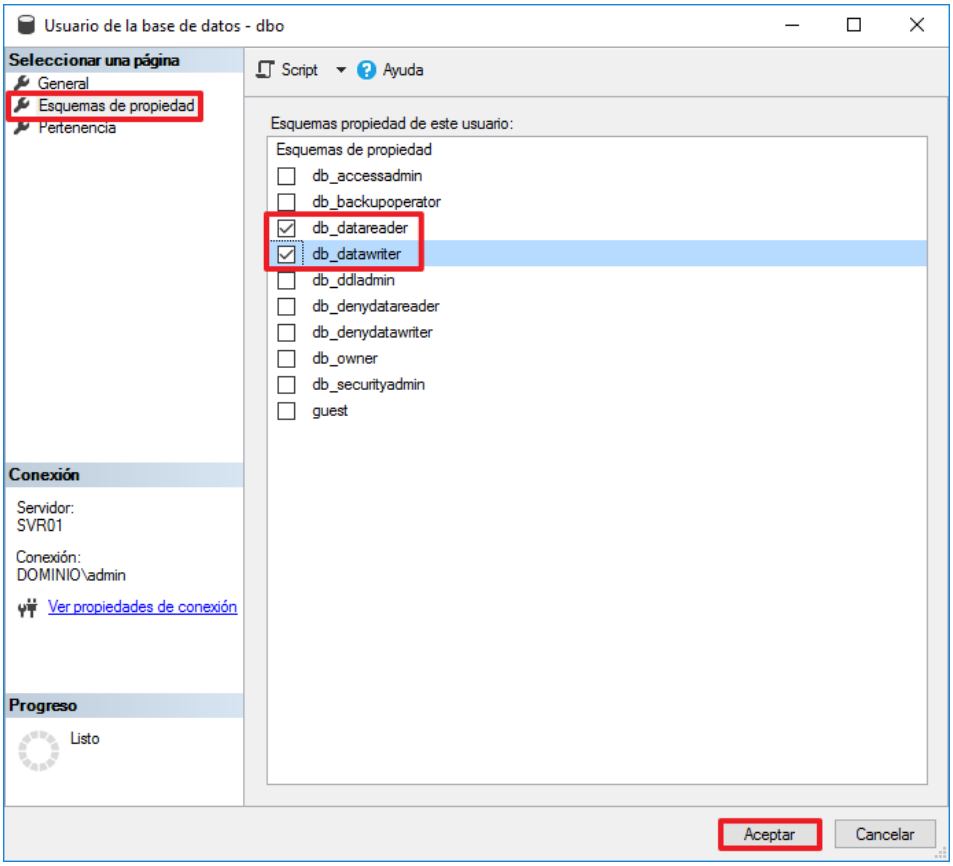
Paso	Descripción
122.	En la siguiente pantalla, seleccione en el menú de la izquierda la página "Permisos" y establezca los permisos necesarios a corde a su organización. Cuando haya finalizado pulse "Aceptar" para guardar los permisos configurados.  **Nota:** SQL Server posee una gestión de usuarios, roles, permisos y políticas sobre los objetos específicos contenidos en la base de datos dentro del servidor SQL. Dicha gestión se puede asignar mediante permisos de seguridad individuales para cada uno de estos objetos. Para más información sobre los permios en SQL Server 2016 consulte la siguiente página: https://docs.microsoft.com/es-es/sql/relational-databases/security/permissions-database-engine?view=sql-server-2016.

2.5.2. PERMISOS DE USUARIOS SOBRE BASES DE DATOS

En esta sección se definen los procesos para alterar los permisos de los diferentes usuarios sobre una base de datos.

Paso	Descripción
123.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.

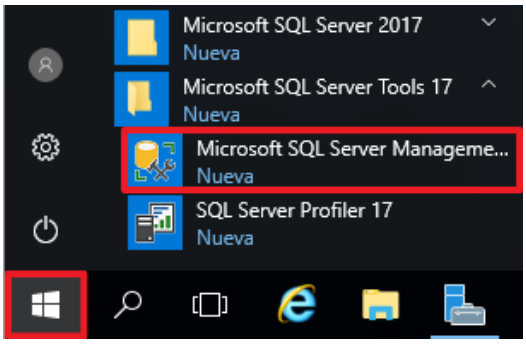
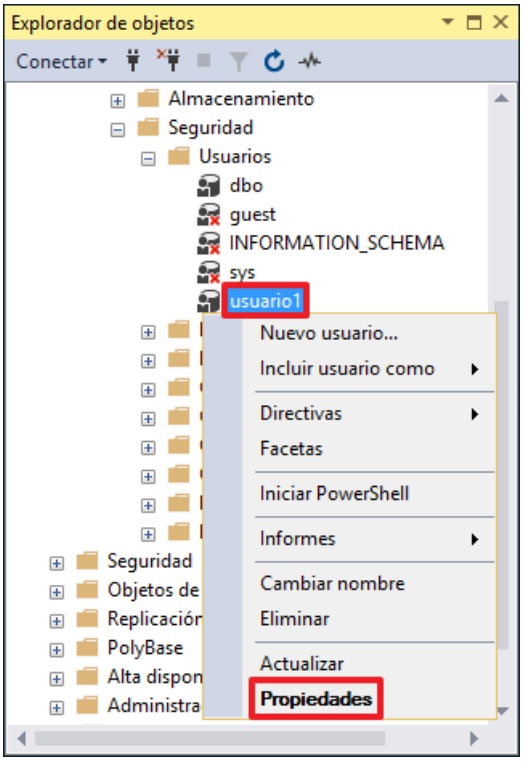
Paso	Descripción
124.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".** 
125.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".
126.	Una vez dentro de la consola de administración de SQL Server, expanda el árbol de su base de datos hasta llegar al siguiente nodo **"Bases de datos → <PRUEBA-BBDD-1> → Seguridad → Usuarios"** y desplegando el menú contextual con el botón derecho sobre el usuario que quiera administrar, seleccione la opción "Propiedades".  **Nota:** En este ejemplo, se utiliza el usuario "dbo" sobre la base de datos "PRUEBA-BBDD-1".

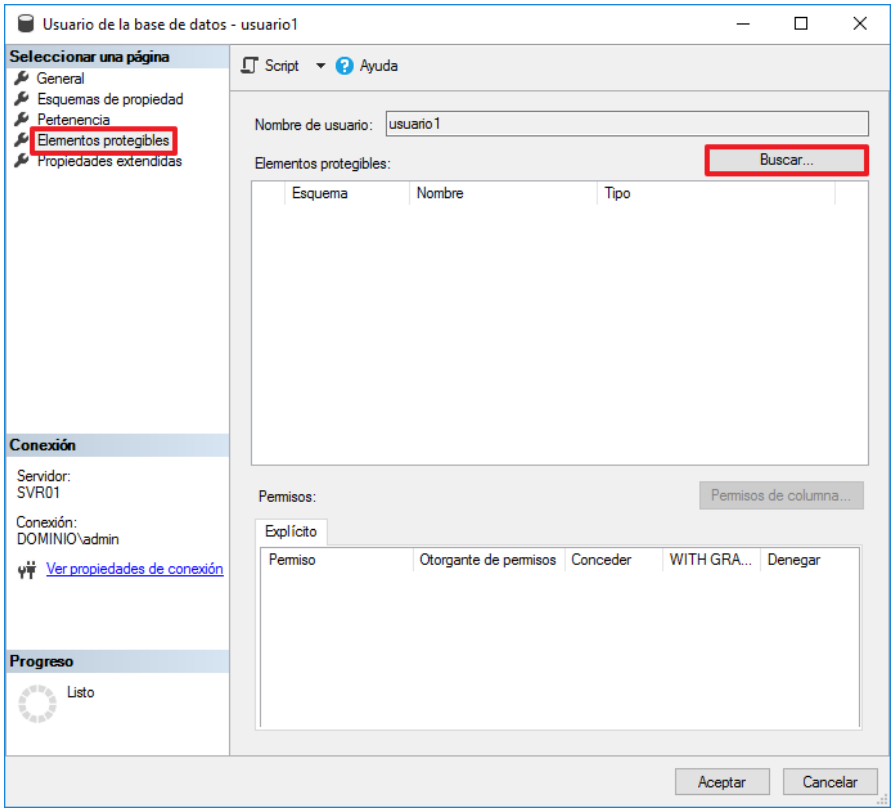
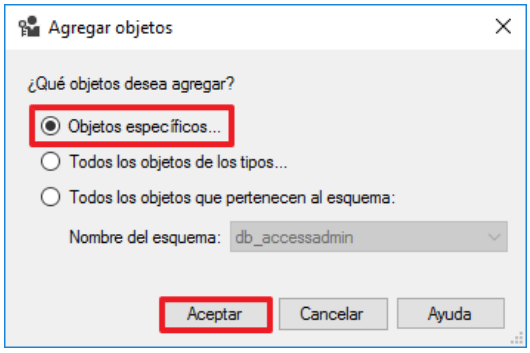
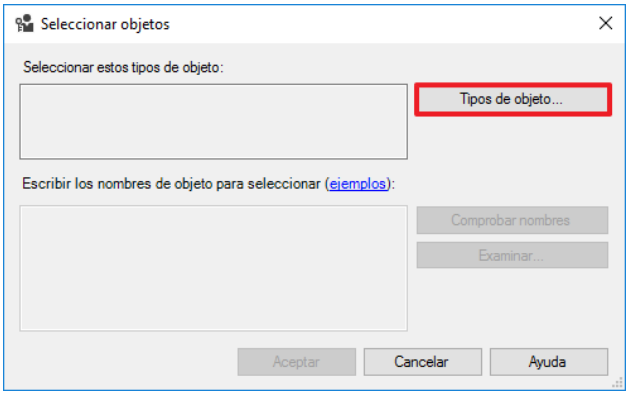
Paso	Descripción
127.	En la siguiente ventana, sitúese en el menú de la izquierda y pinche en la página "Esquemas de propiedad" y asigne los permisos de usuario sobre la base datos acorde a las necesidades de su organización y pulse "Aceptar".  **Nota:** En este ejemplo, se han asignado los permisos de lectura ("db_datareader") y modificación ("db_datawriter").

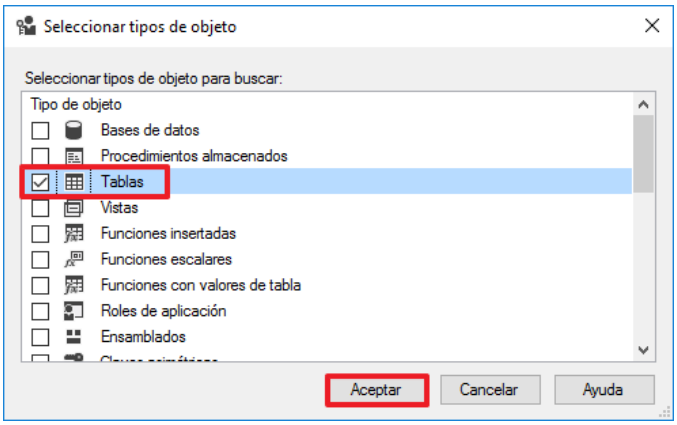
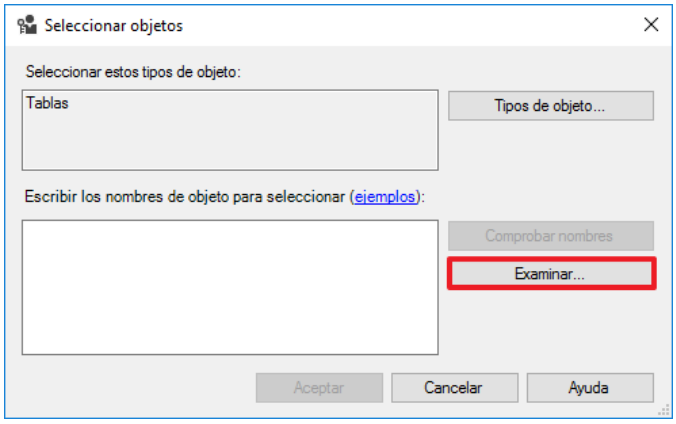
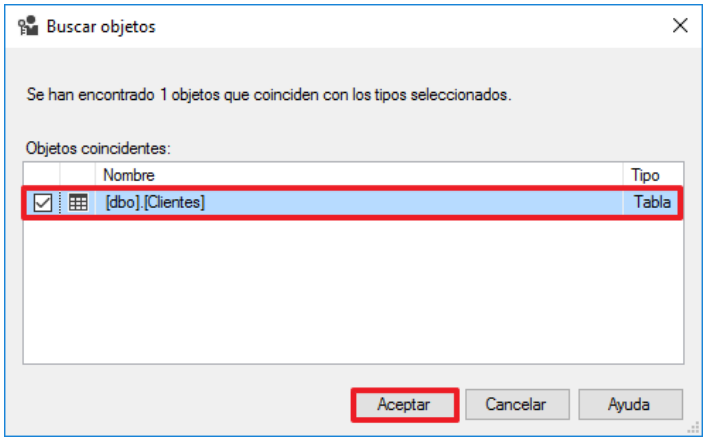
2.5.3. PERMISOS EN TABLAS

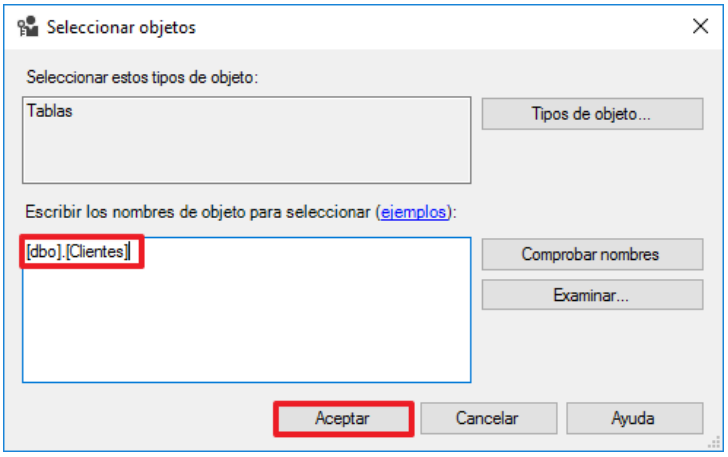
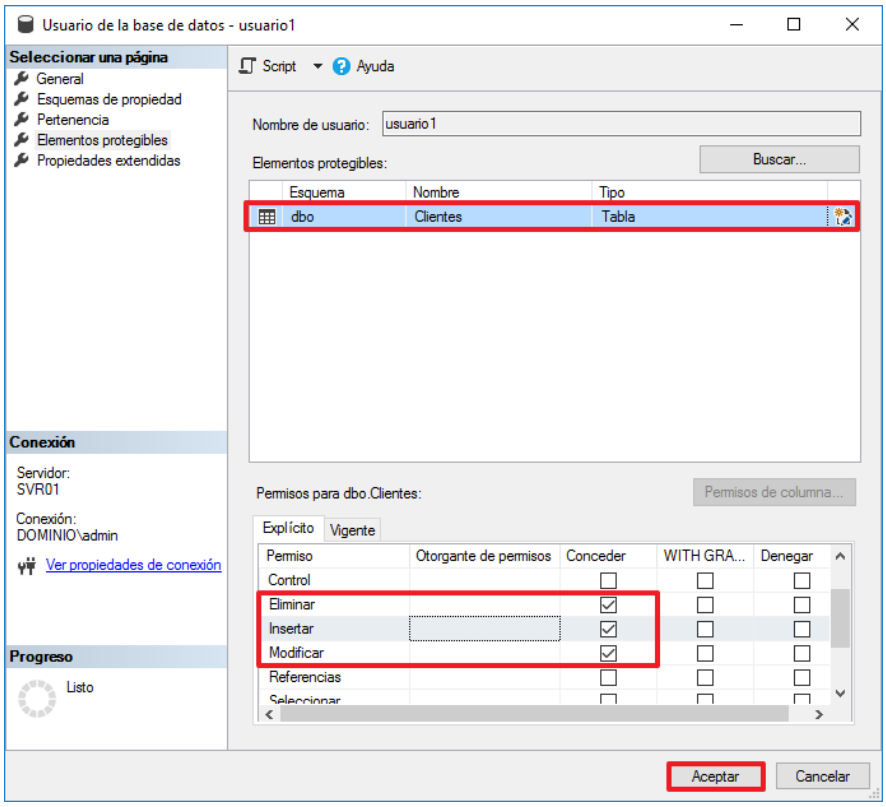
En este procedimiento se describen los procesos para cambiar permisos en las tablas.

Paso	Descripción
128.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.

Paso	Descripción
129.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".** 
130.	En la ventana de "Conectar con el servidor", asegúrese de que el nombre del servidor es el correcto y pulse "Conectar".
131.	Una vez dentro de la consola de administración de SQL Server, expanda el árbol de su base de datos hasta llegar al siguiente nodo **"Bases de datos → <PRUEBA-BBDD-1> → Seguridad → Usuarios"** y desplegando el menú contextual con el botón derecho sobre el usuario que quiera administrar, seleccione la opción "Propiedades".  **Nota:** En este ejemplo, se utiliza el usuario "usuario1" sobre la base de datos "PRUEBA-BBDD-1".

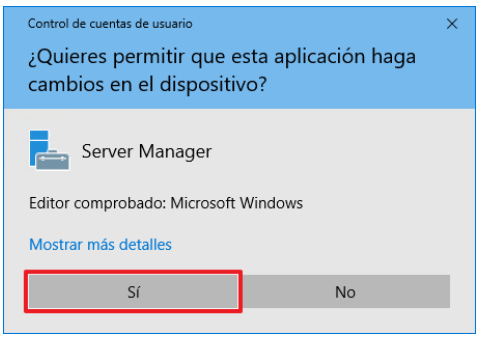
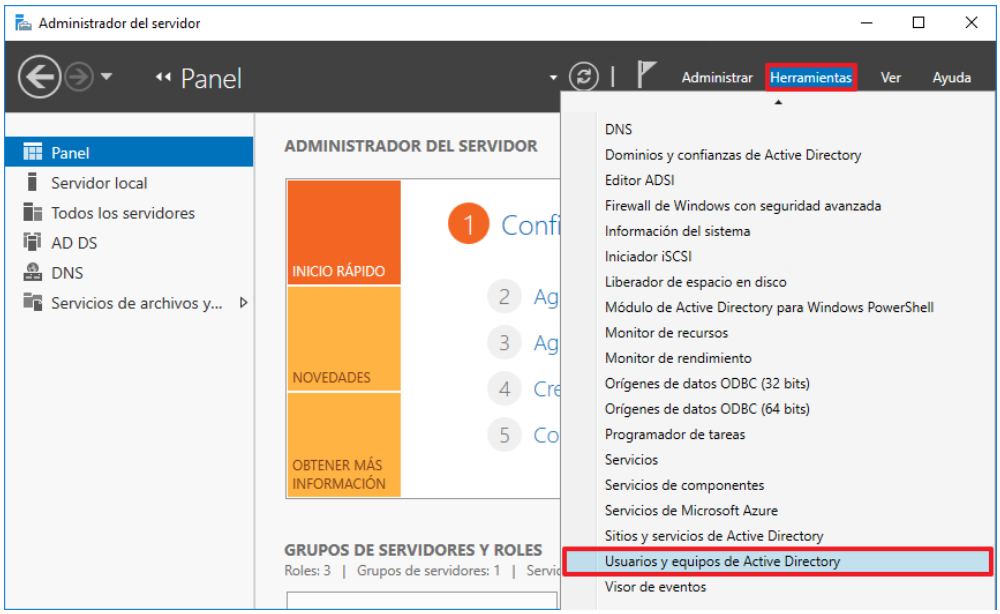
Paso	Descripción
132.	En la siguiente ventana, sitúese en el menú de la izquierda y pinche en la página "Elementos protegibles" y pulse sobre el botón "Buscar…". 
133.	A continuación, seleccione "Objetos específicos…" y pulse "Aceptar". 
134.	En la siguiente ventana emergente, presione "Tipos de objeto…". 

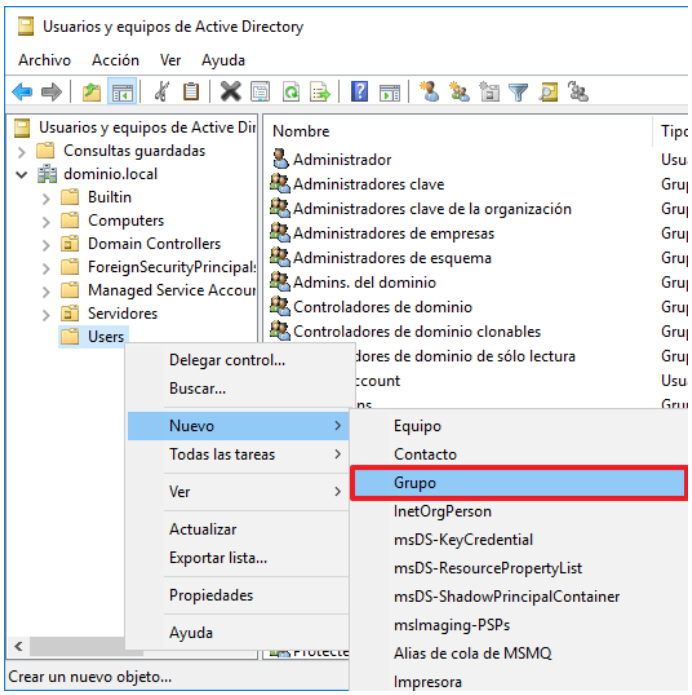
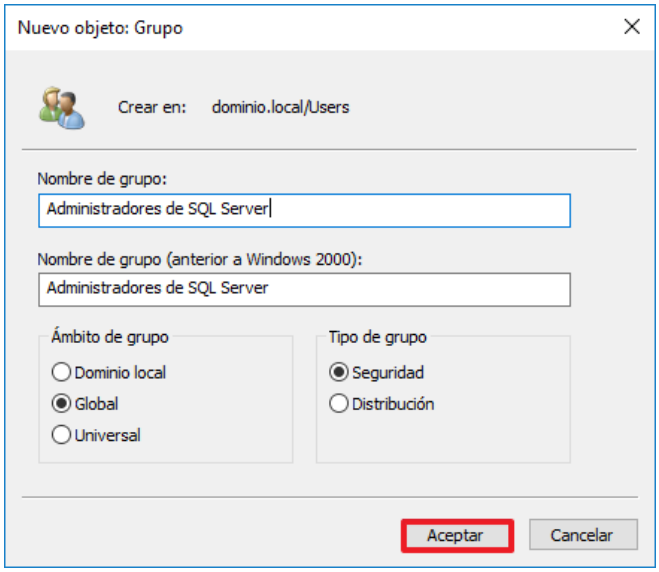
Paso	Descripción
135.	Seleccione el objeto "Tablas" y pulse "Aceptar". 
136.	A continuación, pulse el botón "Examinar…". 
137.	En la siguiente ventana emergente, seleccione la tabla que desea asignarle al usuario previamente establecido. 

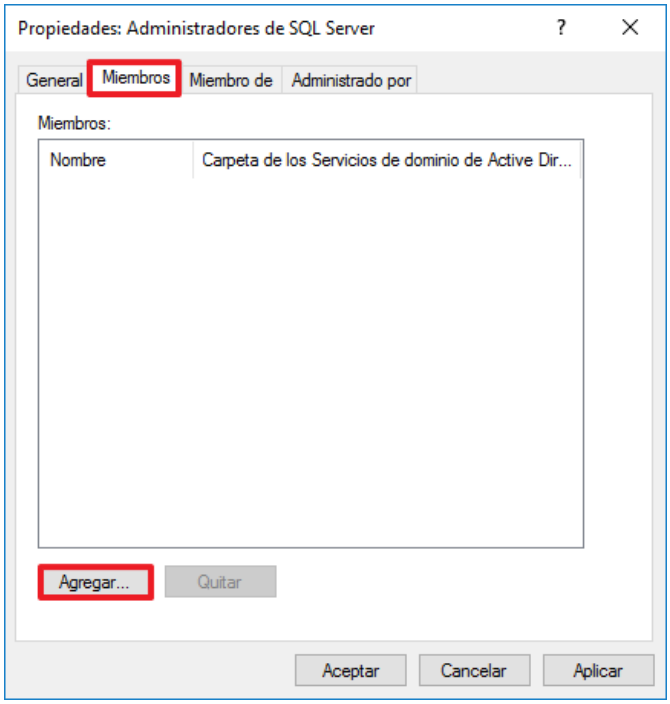
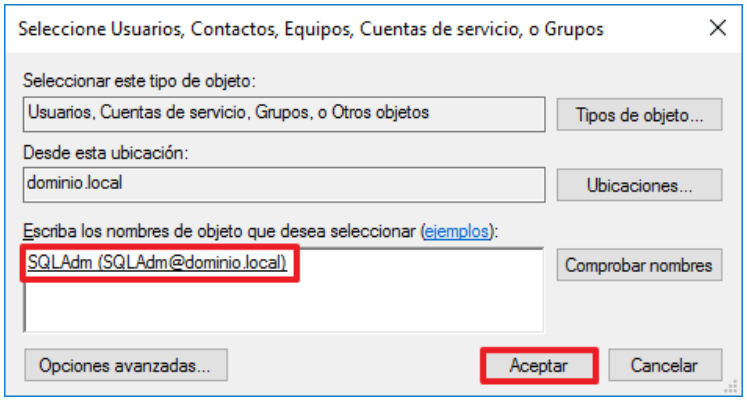
Paso	Descripción
138.	Para finalizar, compruebe que la tabla se ha asignado correctamente y vuelva a pulsar "Aceptar" para guardar los cambios. 
139.	En la parte inferior de la ventana, asigne los permisos al usuario sobre la tabla seleccionada acorde a las necesidades de su organización. Pulse "Aceptar" para guardar los cambios.  **Nota:** En este ejemplo, se han asignado los permisos de eliminar, insertar y modificar al usuario "usuario1" sobre la tabla "Clientes".

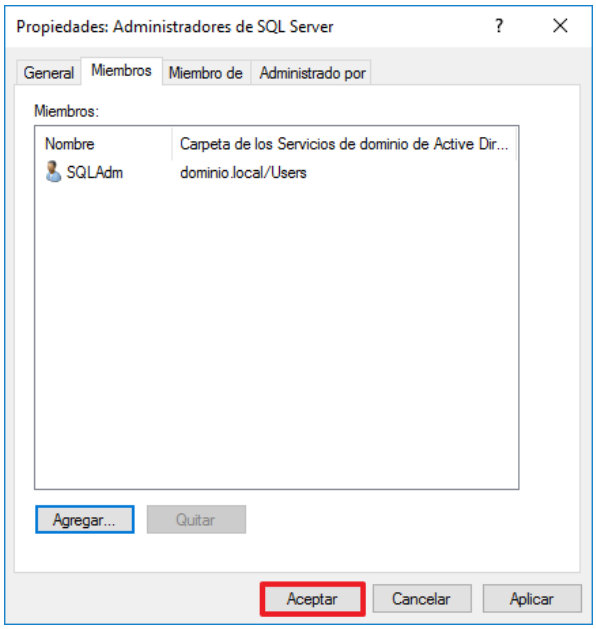
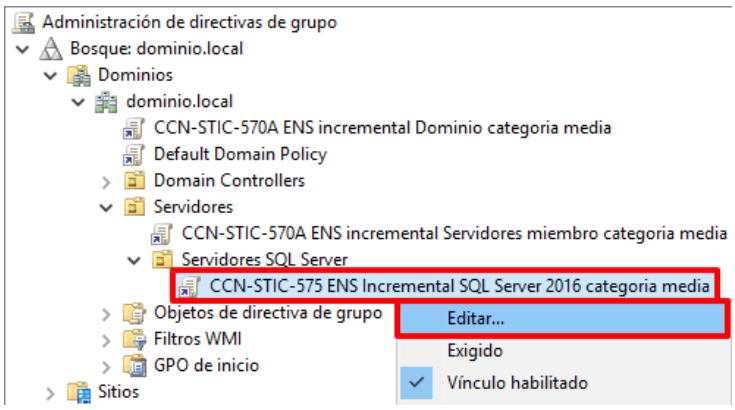
2.6. SEGREGACIÓN DE ROLES

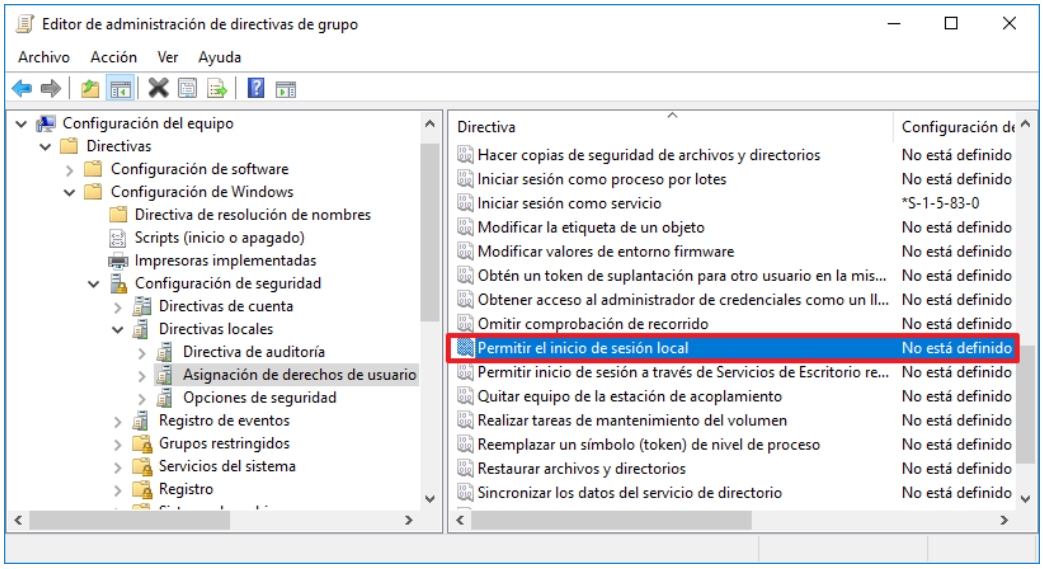
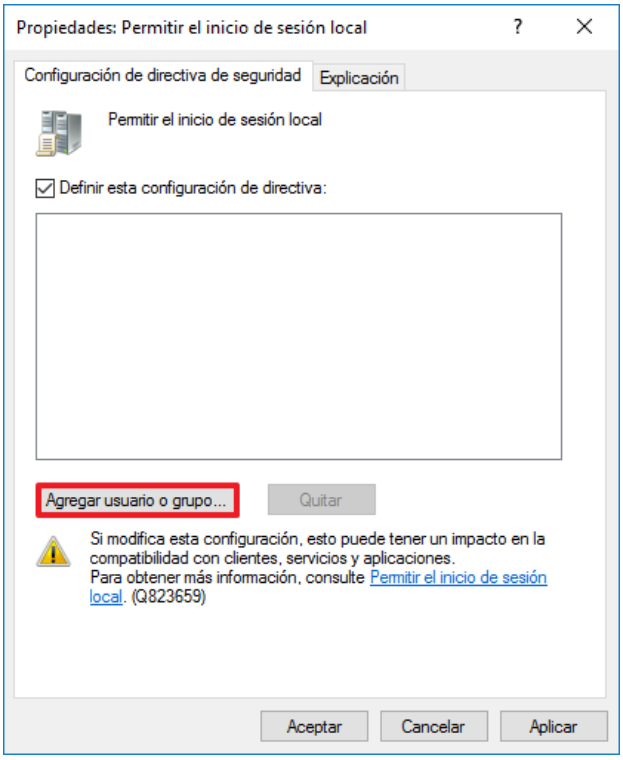
Con la aplicación del ENS para la categoría media sobre un servidor SQL Server 2016 será necesario crear grupos de usuarios para conceder o denegar permisos sobre un recurso, así como administrar SQL Server 2016.

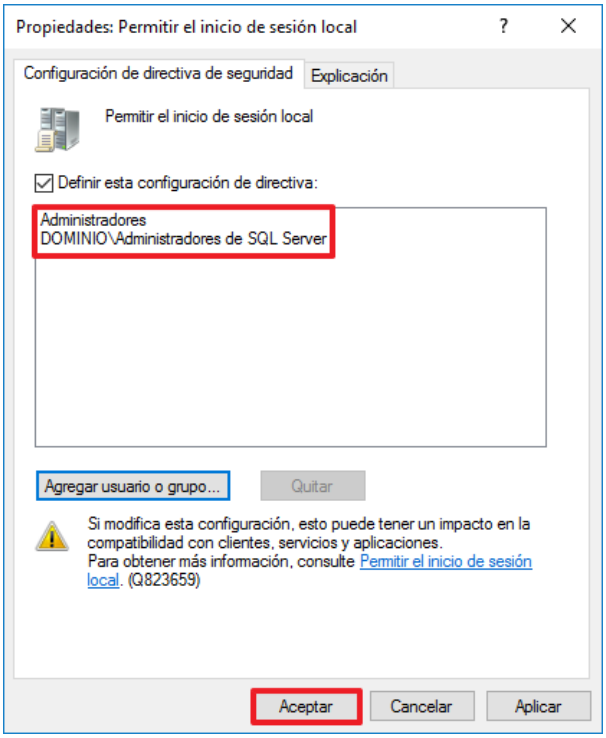
Paso	Descripción
140.	Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad según criterios de ENS. **Nota:** Inicie sesión con una cuenta que sea "Administrador del Dominio".
141.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
142.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
143.	Acceda al apartado "Herramientas" y seleccione "Usuarios y Equipos de Active Directory". 

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

Paso	Descripción
146.	Haga doble clic sobre el grupo recién creado y acceda a la pestaña "Miembros". Pulse sobre el botón "Agregar…" para añadir usuarios al grupo. 
147.	Añada los usuarios que desee al grupo y pulse "Aceptar".  **Nota:** En este ejemplo se añade el usuario "SQLAdm".

Paso	Descripción
148.	Pulse "Aceptar" cuando haya finalizado. 
149.	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".** 
150.	Acceda al nodo "Servidores de SQL Server", pulse con el botón derecho el objeto GPO denominado "CCN-STIC-575 ENS incremental SQL categoria media", creado en apartados anteriores y seleccione la opción del menú contextual "Editar…". 

Paso	Descripción
151.	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"**. 
152.	Marque la casilla "Definir esta configuración de directiva:" y pulse sobre "Agregar usuario o grupo…". 

<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>153.</td><td>Agregue el grupo “Administradores” y aquellos usuarios o grupos delegados para la administración del servidor SLQ Server 2016. Pulse “Aceptar” cuando haya finalizado.


Nota: En este ejemplo se hace uso del grupo denominado “Administración de SQL Server”. Deberá adaptar esta configuración a las necesidades de su organización.</td></tr>
<tr><td>154.</td><td>Repita el proceso nuevamente a partir del paso “152 a 153” para las siguientes directivas:

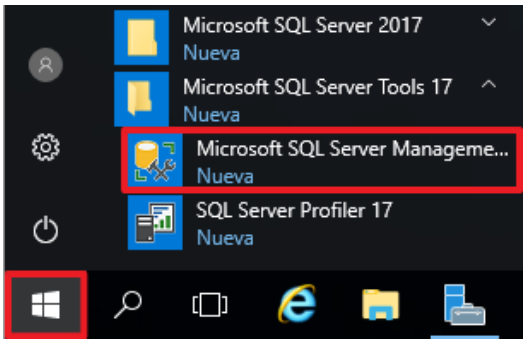
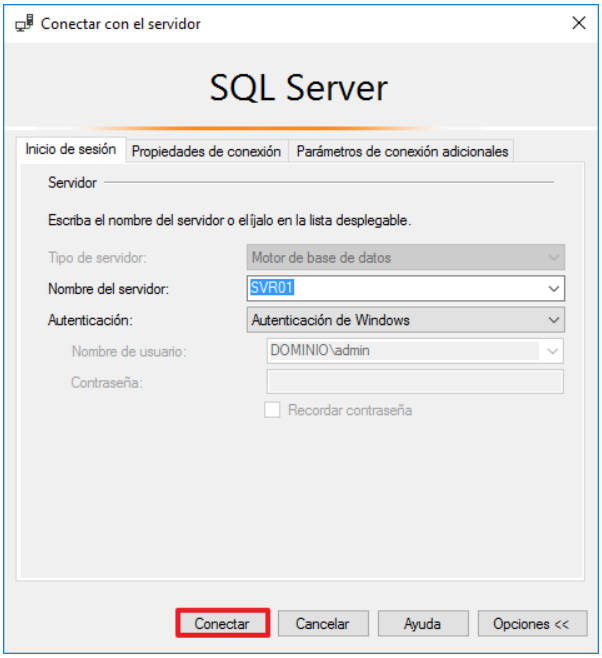
Depurar programas.
Hacer copias de seguridad de archivos y directorios.
Permitir el inicio de sesión local.

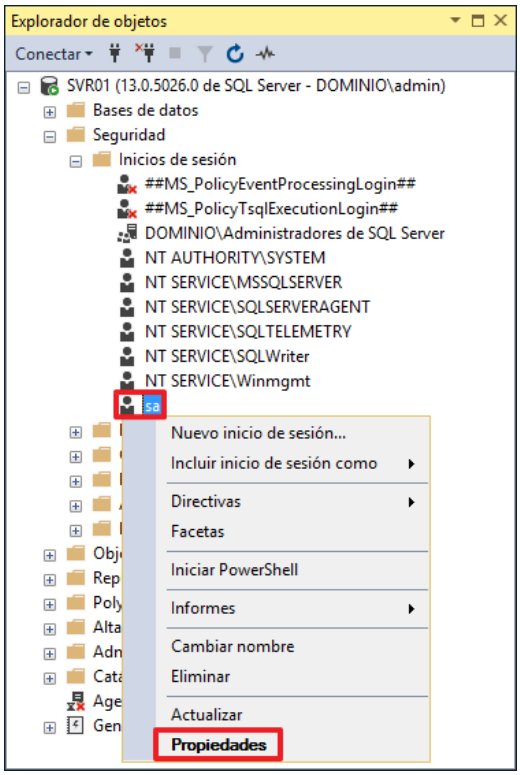
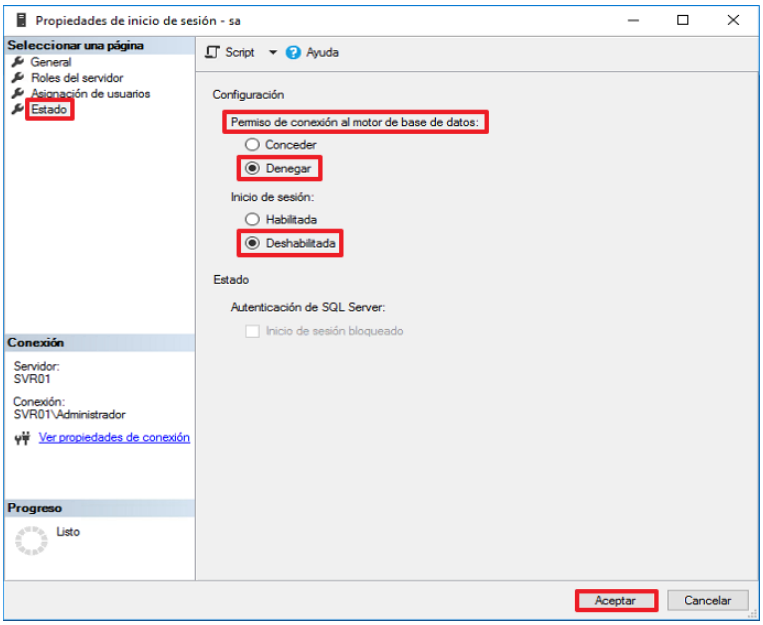
La siguiente tabla muestra cómo deben quedar configuradas las directivas:
<table>
<tr><th>Directiva</th><th>Configuración de directiva</th></tr>
<tr><td>Administrar registro de seguridad y auditoría</td><td>Administradores
DOMINIO\Administradores de SQL Server</td></tr>
<tr><td>Depurar programas</td><td>DOMINIO\Administradores de SQL Server</td></tr>
<tr><td>Hacer copia de seguridad de archivos y directorios</td><td>Administradores
BUILTIN\Operadores de copia de seguridad
DOMINIO\Administradores de SQL Server</td></tr>
<tr><td>Permitir el inicio de sesión local</td><td>Administradores
DOMINIO\Administradores de SQL Server</td></tr>
</table></td></tr>
</table>

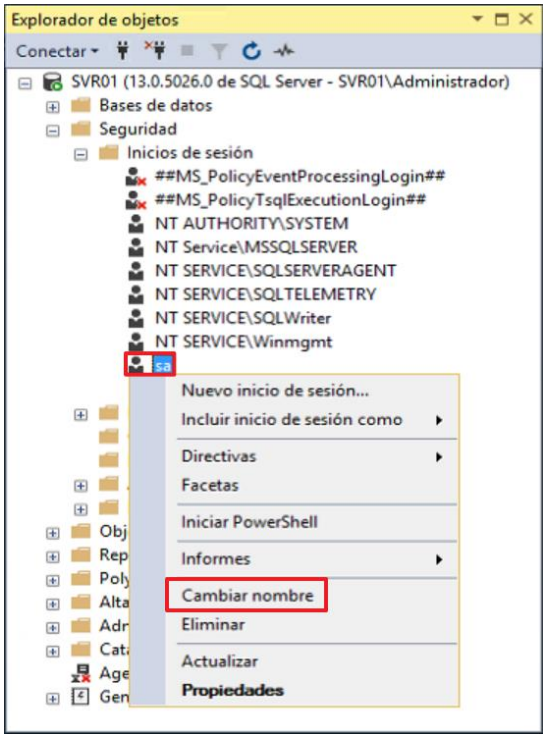
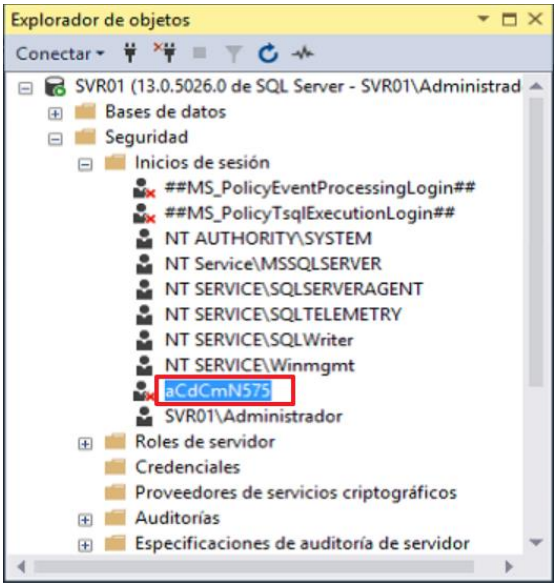
2.7. SEGURIDAD SOBRE EL USUARIO SA

SQL Server 2016 instala de forma predeterminada un inicio de sesión denominado "Sa" como abreviatura de "system administrator" ("administrador de sistema"). El inicio de sesión de "sa" se asigna al rol del servidor sysadmin, con lo que dispone de credenciales administrativas irrevocables en todo el servidor.

Para ello, en el siguiente punto se deshabilitará el inicio de sesión del usuario "sa" y se le asignará un nombre alternativo para impedir ataques de fuerza bruta sobre dicho usuario.

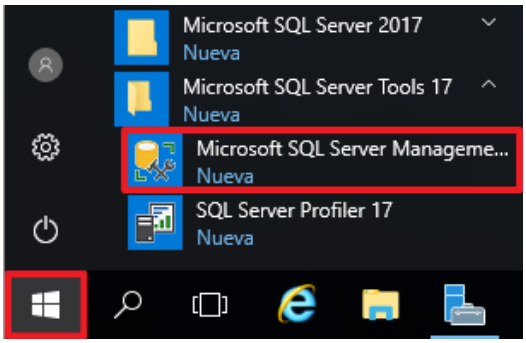
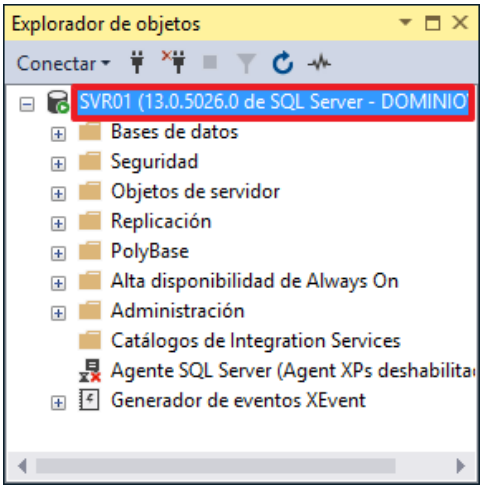
Paso	Descripción
155.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta que pertenezca al grupo "Administradores de SQL Server".
156.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".** 
157.	En la ventana de "Conectar con el servidor", asegúrese de que el nombre del servidor es el correcto y pulse "Conectar". 

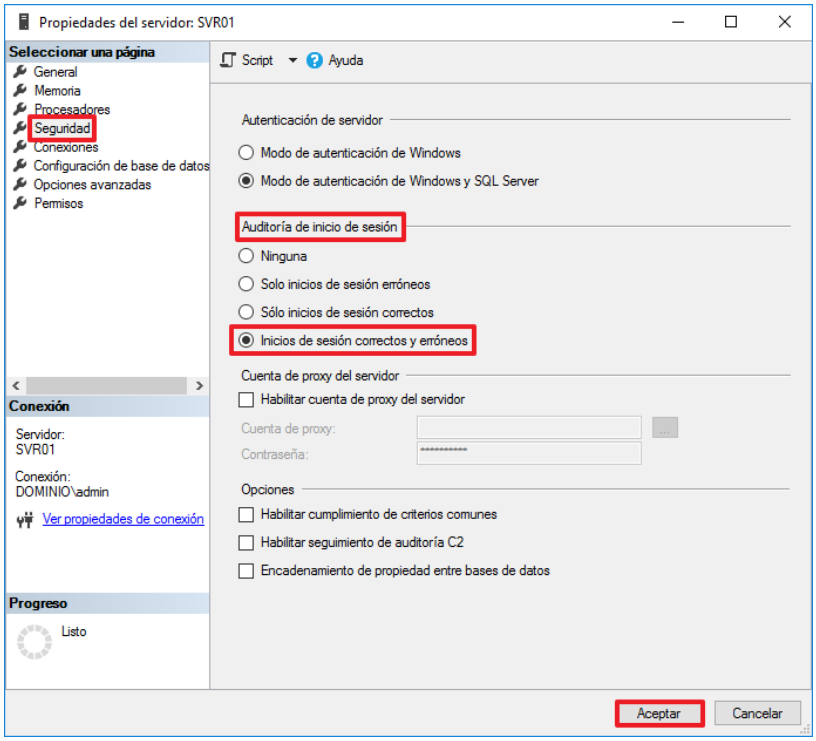
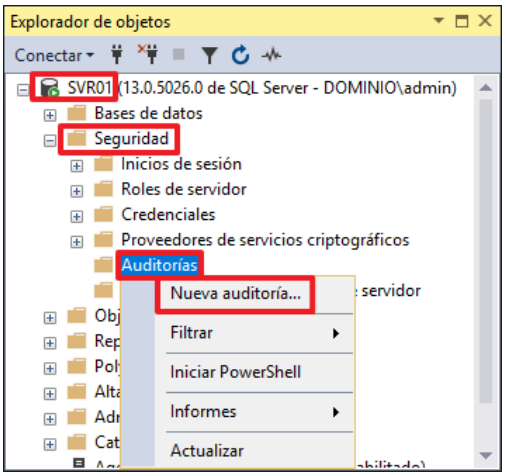
Paso	Descripción
158.	A continuación, despliegue el nodo **"Servidor: <<nombre del servidor>> → Seguridad → Inicios de sesión"** y desplegando el menú contextual con el botón derecho, seleccione la opción "Propiedades".  **Nota:** En este ejemplo, se utiliza el nombre del servidor "SVR01".
159.	A continuación, sitúese en la página "Estado" dentro de la configuración "Permiso de conexión al motor de base de datos" y seleccione "Denegar". Repita el mismo proceso, pero en la configuración "Inicio de sesión" marcando la opción "Deshabilitada". Pulse "Aceptar" para guardar los cambios. 

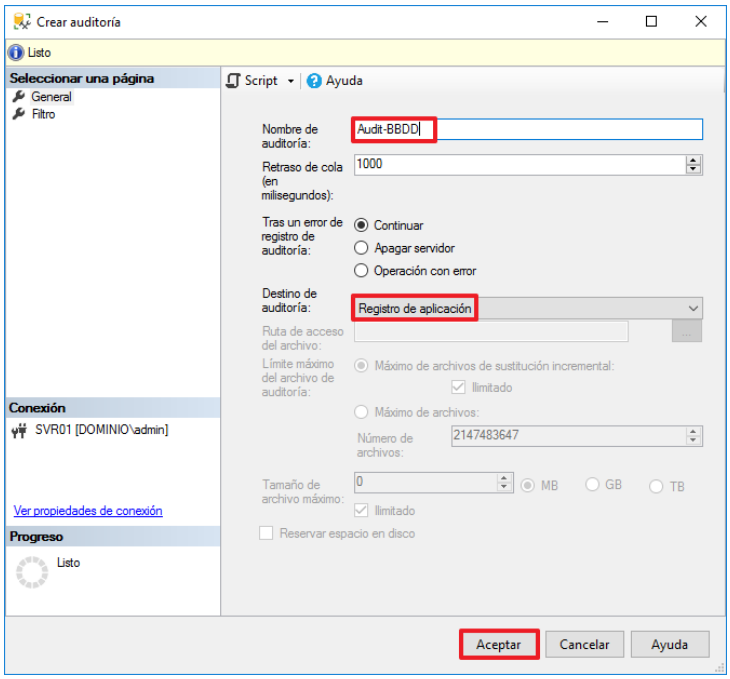
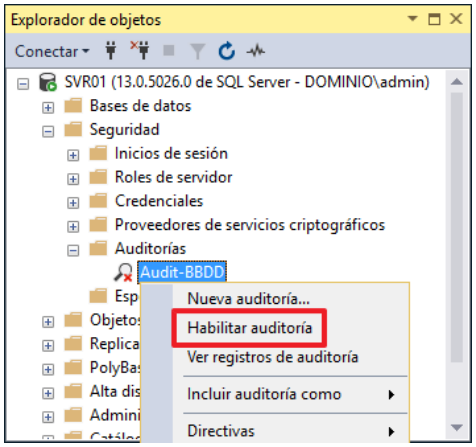
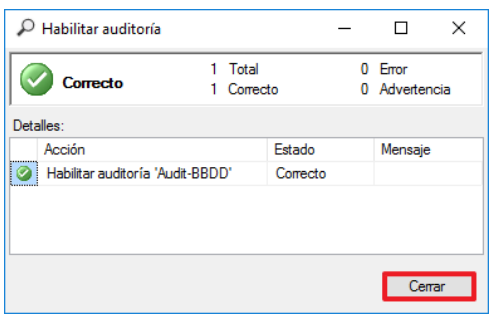
Paso	Descripción
160.	Una vez deshabilitado el usuario "sa", haga clic derecho sobre dicho usuario y desplegando el menú contextual, seleccione la opción "Cambiar nombre".  **Nota:** Verifique que el usuario "sa" aparece deshabilitado mediante una "X" de color rojo. Si no es así, pulse F5 para refrescar el explorador de objetos.
161.	Establezca el nombre "aCdCmN575" para el usuario "sa". 

2.8. AUDITORÍA EN SQL SERVER 2016

Existe la posibilidad que auditores lleven un control de las diferentes tareas que se realizan a través de SQL Server 2016. Esta sección recoge los pasos a seguir para realizar la configuración de una auditoria de eventos de un servidor de SQL Server 2016. Estos pasos se realizarán a través de un servidor SQL Server 2016.

Paso	Descripción
162.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
163.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
164.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".
165.	Dentro del Explorador de objetos, seleccione su servidor de SQL Server y haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Propiedades". 

Paso	Descripción
166.	En la siguiente pantalla, seleccione en el menú de la izquierda la página "Seguridad" y en el apartado de "Auditoria de inicio de sesión" marque la opción "Inicios de sesión correctos y erróneos". Cuando haya finalizado pulse "Aceptar" para guardar los permisos configurados. 
167.	A continuación, despliegue el nodo **"Servidor: <<nombre del servidor>> → Seguridad → Auditorías"** y desplegando el menú contextual con el botón derecho, seleccione la opción **"Nueva auditoria".**  **Nota:** En este ejemplo se utiliza el servidor con el nombre "SVR01".

Paso	Descripción
168.	En la siguiente ventana de auditoria, establezca un nombre para el registro de auditoria y defina el parametro "Registro de aplicación" como destino de auditoria. Pulse "Aceptar" para guardar los cambios.  **Nota:** En este ejemplo se utiliza el nombre de auditoria "Audit-BBDD".
169.	Ahora, seleccione la auditoria recien creda y desplegando el menú contextual con el botón derecho, seleccione la opción "Habilitar auditoria". 
170.	Una vez finalizado el proceso, verifique que el estado sea correcto y pulse "Cerrar". 

ANEXO A.3.2. LISTA DE COMPROBACIÓN DE SQL SERVER 2016 SOBRE WINDOWS SERVER 2016 PARA SERVIDORES QUE LES SON 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 para SQL Server 2016 sobre Microsoft Windows Server 2016 con implementación de seguridad de categoría básica 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 la sección de la guía "ANEXO A.3.1 PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE MS SQL SERVER 2016 SOBRE SERVIDORES WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS.

1. COMPROBACIONES EN CONTROLADOR DE DOMINIO

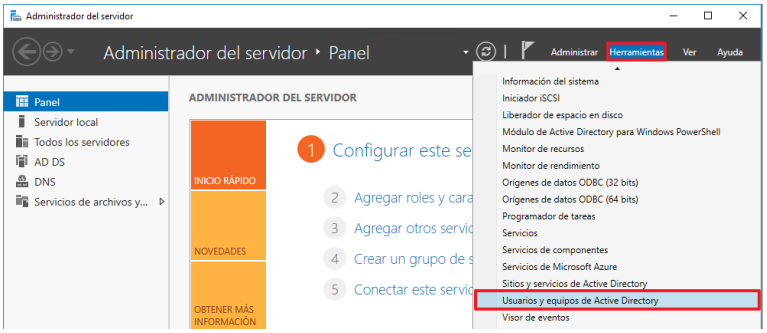
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador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

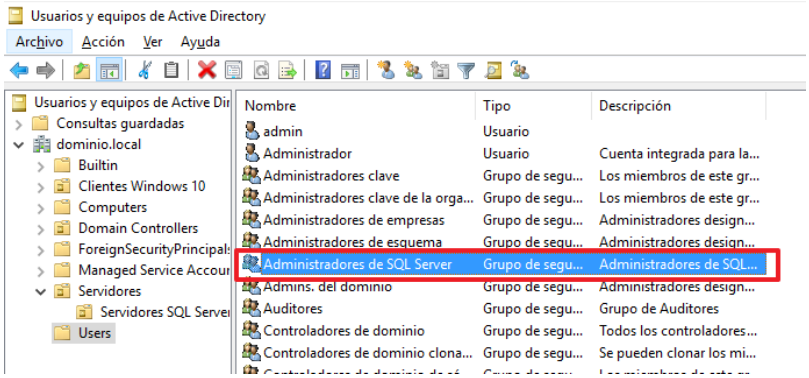
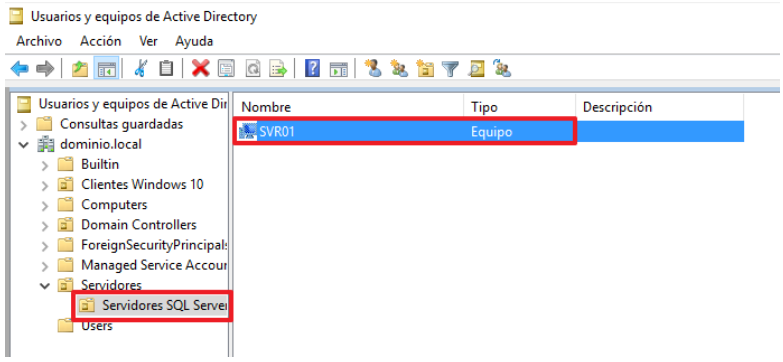
a) Usuarios y equipos de Active Directory (dsa.msc).

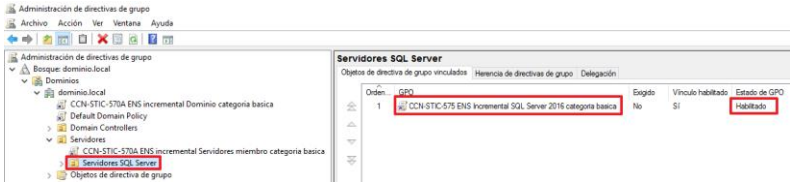
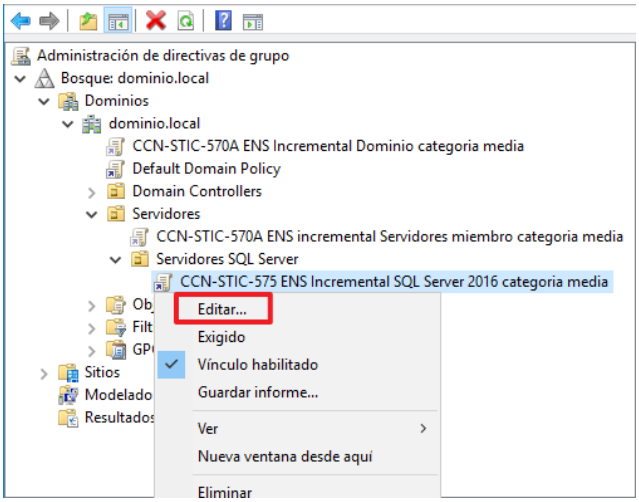
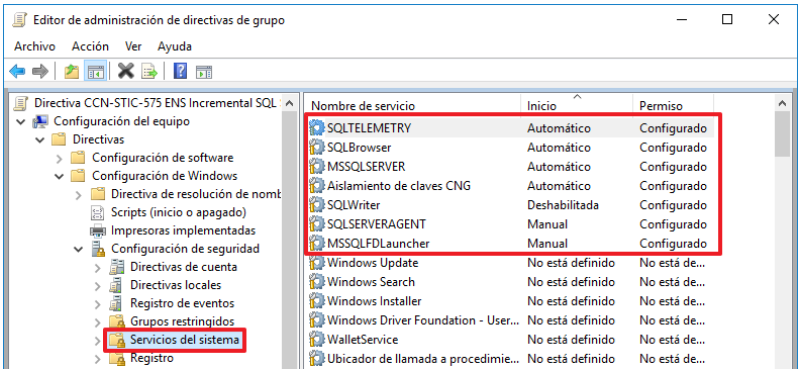
b) Administrador de directivas de grupo (gpmc.msc).

c) Editor de objetos de directiva de grupo (gpedit.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 el servidor controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
2. Verifique que está creado el grupo "Administradores de SQL Server" dentro del contenedor "Users".		Ejecute la herramienta "Usuarios y equipos de Active Directory". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Usuarios y equipos de Active Directory"** 

Comprobación	OK/NOK	Cómo hacerlo
		Seleccione el contenedor "Users", situado en la siguiente ruta: "**Usuarios y equipos de Active Directory → [Su dominio] → Users**" A continuación, en el panel de la derecha, verifique que está creado el objeto denominado "Administradores de SQL Server". 
3. Verifique que los servidores que tienen SQL Server instalado están dentro del contenedor "Servidores SQL Server".		Utilizando la misma consola de "Usuarios y Equipos de Directorio Activo" **(Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory).** Seleccione la unidad organizativa "**Servidores → Servidores SQL Server**", y verifique que existe un objeto de tipo "Equipo" que corresponde al servidor donde se ha instalado SQL Server 2016.  **Nota:** En este ejemplo se ha utilizado la cuenta de equipo SVR01. En su organización los nombres pueden variar.
4. Verifique que los objetos de directivas de grupo han sido creados y están habilitados.		Ejecute la herramienta "Administrador de directivas de grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"** 

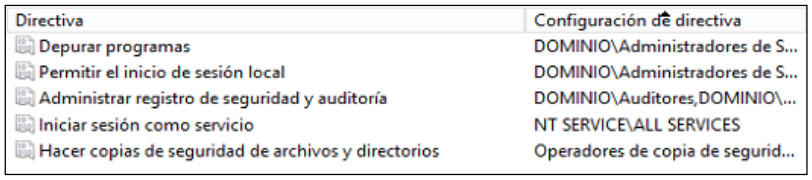
Comprobación	OK/NOK	Cómo hacerlo
		Dentro de la consola diríjase a los "Objetos de directiva de grupo": **"Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo"** Verifique que está creado el objeto de directiva de grupo "CCN-STIC-575 ENS Incremental SQL Server 2016 categoria media" y que en la columna "Estado de GPO" figura como habilitado. 
5. Verifique los servicios del sistema de la directiva SQL Server (CCN-STIC-575 Incremental SQL Server 2016 categoria media).		Seleccionando dicha directiva, pinche sobre ella con el botón derecho y seleccione la opción "Editar" del menú contextual, se abrirá la herramienta "Editor de administración de directiva de grupo" que permitirá verificar los valores de la directiva "CCN-STIC-575 ENS Incremental SQL Server 2016 categoria media".  Verifique que la directiva tiene los siguientes valores en servicios del sistema. Para ello, navegue hasta: **"Directiva CCN-STIC-575 ENS Incremental SQL Server 2016 categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del Sistema"** 

Comprobación	OK/NOK	Cómo hacerlo

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Aislamiento de claves CNG	KeyIso	Automático	Configurado	
SQL Server (MSQLSERVER)	MSSQLSERVER	Automático	Configurado	
SQL Server Browser	SQLBrowser	Automático	Configurado	
SQL Server CEIP service (MSSQLSERVER)	SQLTELEMETRY	Automático	Configurado	
SQL Server VSS Writer	SQLWriter	Deshabilitada	Configurado	
SQL Full-Text Filter Daemon Launcher	MSSQLFDLauncher	Manual	Configurado	
Agente SQL Server (MSSQLSERVER)	SQLSERVERAGENT	Manual	Configurado	

6. Verificación derechos de usuarios.

Utilizando el editor de directiva de grupo, verifique que la directiva "CCN-STIC-575 ENS Incremental SQL Server 2016 categoria media" tiene los siguientes valores en las directivas de asignación de derechos de usuario dentro de:
Directiva → CCN-STIC-575 ENS Incremental SQL Server 2016 categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario.



Nota: Verifique que los permisos hayan quedado de la siguiente manera.

Directiva	Valor	OK/NOK
Administrar registro de seguridad y auditoría.	DOMINIO\Administradores de SQL Server, Administradores	
Depurar programas.	DOMINIO\Administradores de SQL Server	
Hacer copias de seguridad de archivos y directorios.	DOMINIO\Administradores de SQL Server, Administradores, Operadores de copia de seguridad	
Iniciar sesión como servicio.	NT SERVICE\ALL SERVICES	
Permitir el inicio de sesión local.	Administradores	

2. COMPROBACIONES EN EL SERVIDOR SQL SERVER 2016

Para realizar esta lista de comprobación primero deberá iniciar sesión en un servidor miembro de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

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

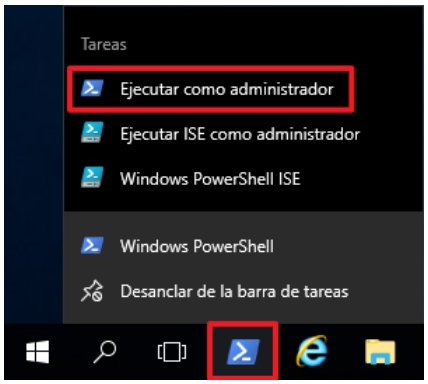
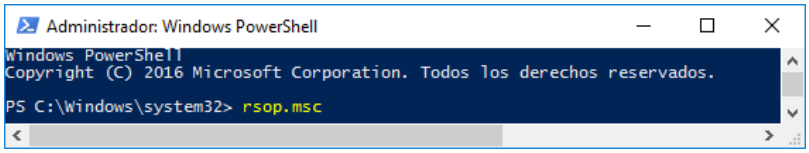
Las consolas y herramientas que se utilizarán son las siguientes:

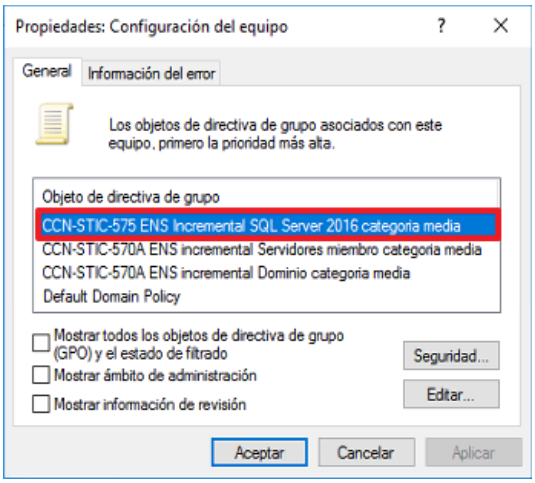
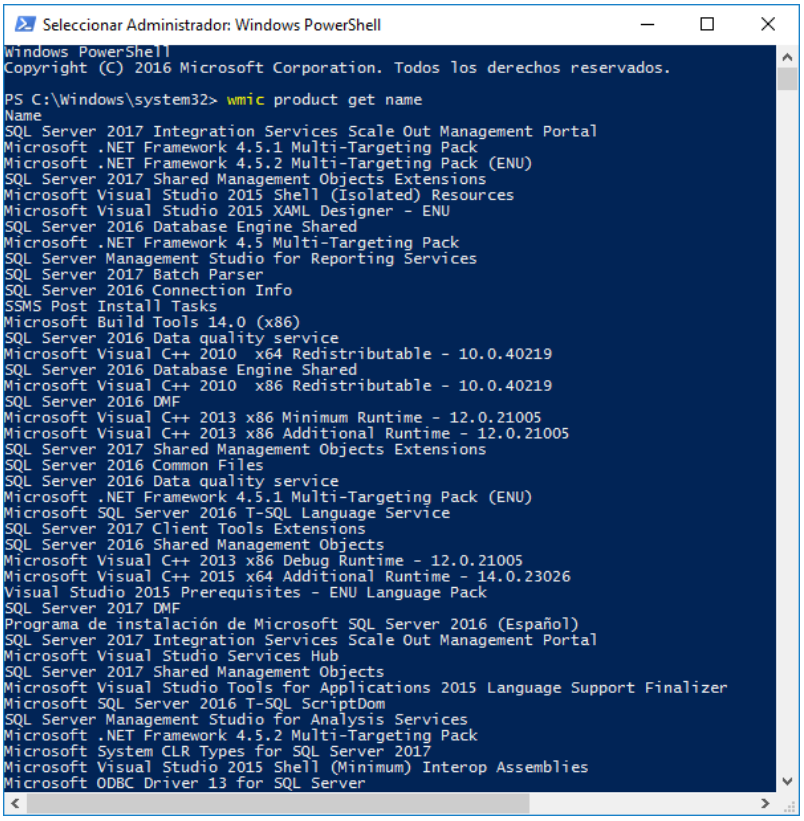
a) Conjunto resultante de directivas (rsop.msc).

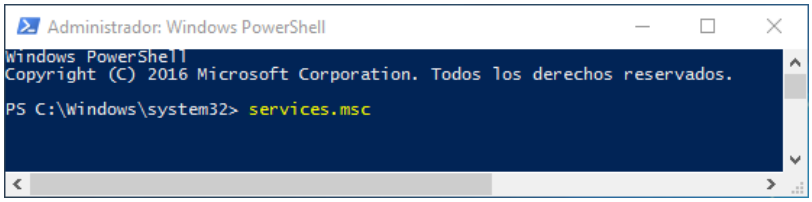
b) Servicios (services.msc).

c) Consola "SQL Server Management Studio".

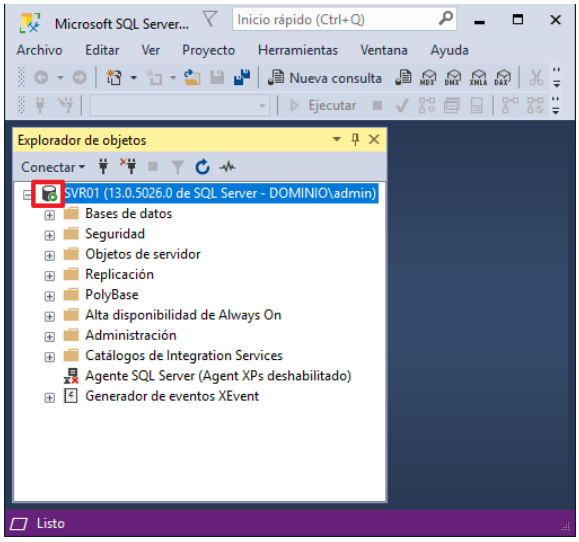
d) Consola "Administrador de configuración de SQL Server".

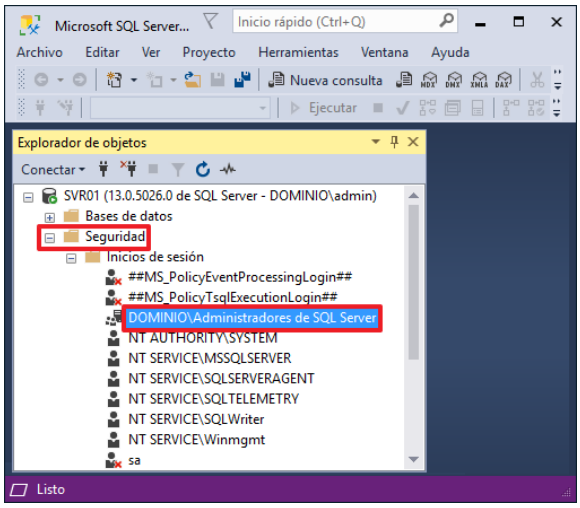
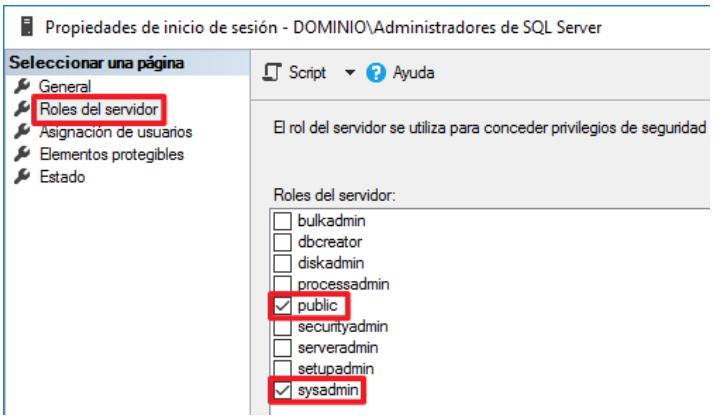
Comprobación	OK/NOK	Cómo hacerlo
7. Inicie sesión en el servidor de SQL Server 2016.		Inicie sesión en el servidor donde se ha implementado el servicio de Microsoft SQL Server 2016 con una cuenta que tenga privilegios de administración del dominio.
8. Verifique la correcta aplicación de la política "CCN-STIC-575 Incremental SQL Server 2016 categoria media" en un equipo miembro del dominio.		Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:  El sistema solicitará elevación de privilegios para poder ejecutar una sesión de PowerShell como administrador. Pulse "Sí" en la ventana de "Control de cuentas de usuario". Teclee "rsop.msc" en la consola de comandos que se ha abierto: 

Comprobación	OK/NOK	Cómo hacerlo
		A continuación, haga clic derecho sobre "Configuración de equipo" en la consola de "Conjunto resultante de directivas" y compruebe que la política "CCN-STIC-575 Incremental SQL Server 2016 categoria media" aparece en la lista como muestra la imagen. 
9. Verifique que SQL Server se ha instalado correctamente.		Teclee "Wmic Product Get Name" en la consola de comandos que se ha abierto anteriormente, y compruebe que aparecen al menos los siguientes productos de SQL Server que se muestran en la siguiente imagen. 

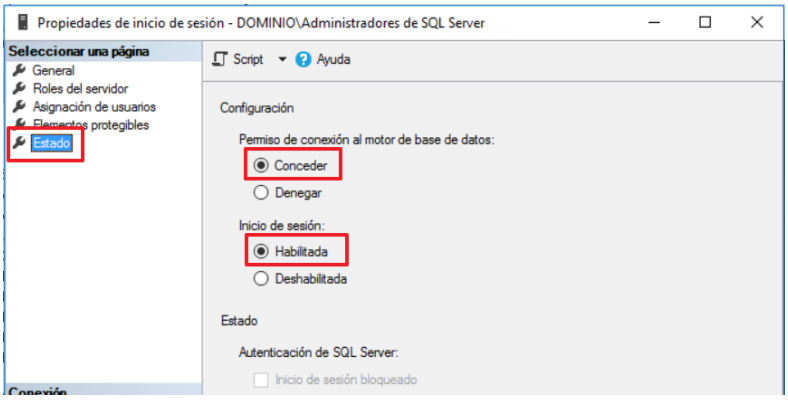
Comprobación	OK/NOK	Cómo hacerlo
10. Verifique la correcta aplicación de la configuración de servicios del sistema de la política "CCN-STIC-575 Incremental SQL Server 2016 categoria media".		Teclee "services.msc" en la consola de comandos que se ha abierto anteriormente:  En la consola de "Servicios", compruebe los siguientes valores.

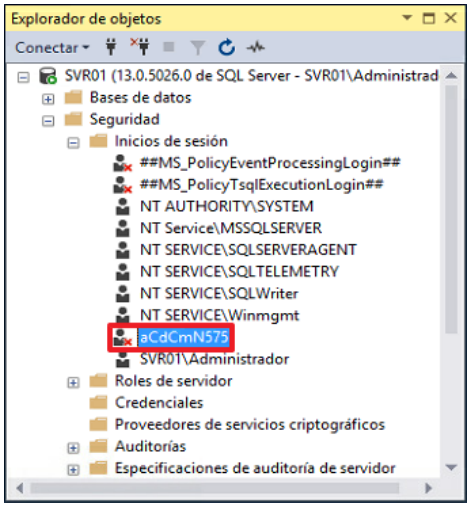
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Aislamiento de claves CNG	KeyIso	Automático	Configurado	
SQL Server (MSQLSERVER)	MSSQLSERVER	Automático	Configurado	
SQL Server Browser	SQLBrowser	Automático	Configurado	
SQL Server CEIP service (MSSQLSERVER)	SQLTELEMETRY	Automático	Configurado	
SQL Server VSS Writer	SQLWriter	Deshabilitada	Configurado	
SQL Full-Text Filter Daemon Launcher	MSSQLFDLauncher	Manual	Configurado	
Agente SQL Server (MSSQLSERVER)	SQLSERVERAGENT	Manual	Configurado	

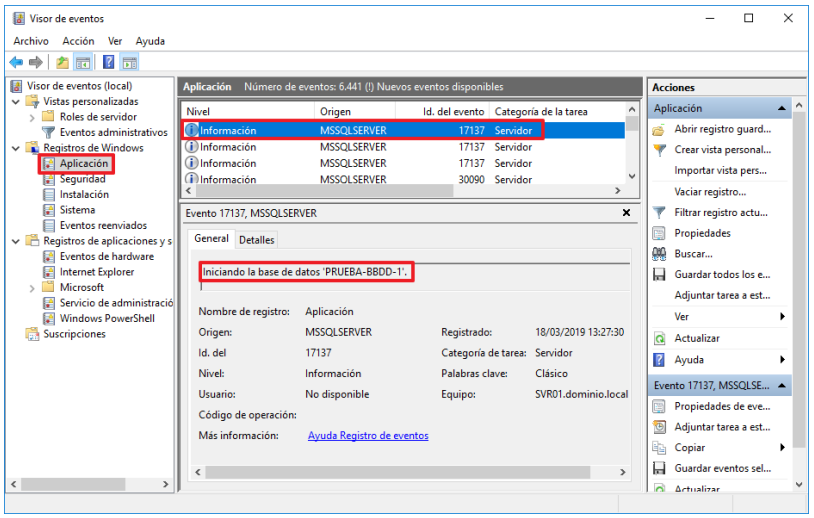
11. Verifique la correcta conexión con el servicio de SQL Server desde la consola de administración.		Utilizando la consola de administración de SQL Server Management 17 (**"Inicio → Microsoft SQL Server Tools 17 → SQL Server Management Studio 17"**). Compruebe que se puede conectar correctamente al nombre del servidor que ejecuta el motor de bases de datos de SQL Server.  **Nota:** En este ejemplo se utiliza el nombre "SVR01.dominio.local".

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>12. Verifique que el grupo de seguridad global “Administradores de SQL Server” está registrado en la consola de administración de SQL Server.</td><td></td><td>Utilizando la consola de administración de SQL 2016 (“Inicio → Microsoft SQL Server Tools 17 → SQL Server Management Studio 17”).
Compruebe que el grupo de dominio denominado “Administradores de SQL Server” esté configurado como inicio de sesión.
Navegue hasta el nodo “Seguridad → Inicio de sesión” y compruebe que existe el grupo “DOMINIO\Administradores de SQL Server”.
 
</td></tr>
<tr><td>13. Verifique los privilegios de roles del servidor para el grupo “Administradores de SQL Server”</td><td></td><td>Utilizando la consola de administración de SQL 2016 (“Inicio → Microsoft SQL Server Tools 17 → SQL Server Management Studio 17”).
Compruebe que el grupo de dominio denominado “Administradores de SQL Server” dispone de los permisos adecuados para administrar SQL Server.
Con el botón derecho seleccione el grupo “DOMINIO\Administradores de SQL Server” y haga clic en la opción del menú contextual “Propiedades”. A continuación, seleccione “Roles del servidor” y compruebe que están habilitados los roles “Sysadmin” y “Public”.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Public</td><td>Habilitado</td><td></td></tr>
<tr><td>Sysadmin</td><td>Habilitado</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>14. Verifique que el grupo de seguridad global “Administradores de SQL Server” tiene habilitado el inicio de sesión.</td><td></td><td>Utilizando la consola de administración de SQL 2016 (Inicio → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17).
Compruebe que el grupo de dominio denominado “Administradores de SQL Server” tiene habilitado el inicio de sesión.
Con el botón derecho seleccione el grupo “DOMINIO\Administradores de SQL Server” y haga clic en la opción del menú contextual “Propiedades”. A continuación, seleccione “Estado” y verifique que el permiso de conexión al motor de base de datos esté concedido y que el inicio de sesión esté habilitado.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Permiso de conexión al motor de base de datos</td><td>Conceder</td><td></td></tr>
<tr><td>Inicio de sesión</td><td>Habilitado</td><td></td></tr>
</table></td></tr>
<tr><td>15. Verifique la correcta conexión con el servicio de SQL Server desde la consola de administración.</td><td></td><td>Dentro del Explorador de archivos, despliegue el nodo “Servidor: <<nombre del servidor>> → Seguridad → Inicios de sesión” y compruebe que el usuario “sa”, previamente renombrado como “aCdCmN575”, se encuentra deshabilitado.
 
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
16. Verifique que la auditoría sobre el servidor de SQL Server 2016 se encuentra activada		Utilizando la herramienta de visor de eventos de Windows (ejecutando "eventvwr.msc" desde **Inicio → Ejecutar…**), verifique que la auditoría del servidor del servidor de SQL Server 2016 se encuentra activada en el registro de Aplicación. 

ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.4.1. PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE MS SQL SERVER 2016 SOBRE SERVIDORES WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA 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 SQL Server 2016 con una categorización de seguridad alta según los criterios del Esquema Nacional de Seguridad.

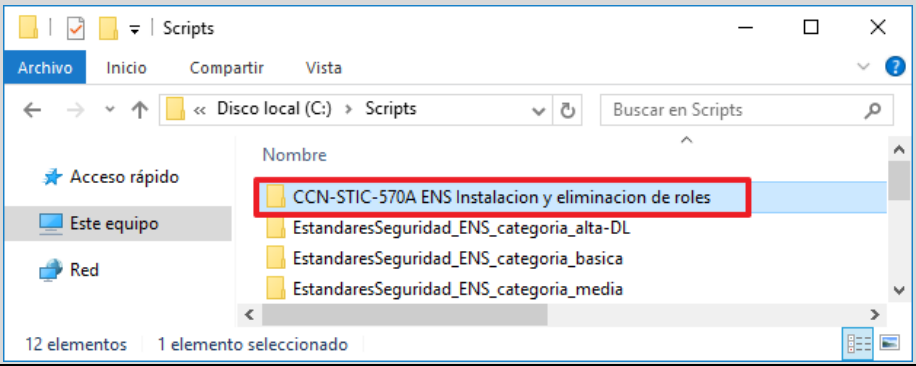
Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios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

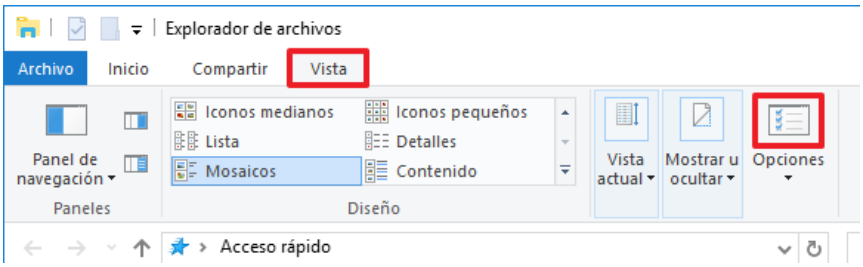
Nota: Si instala SQL Server 2016 por primera vez con la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016 aplicada debe habilitar la instalación remota de roles características y servicios de rol a través de Shell la cual se encuentra deshabilitada por GPO.
En la guía mencionada anteriormente 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.

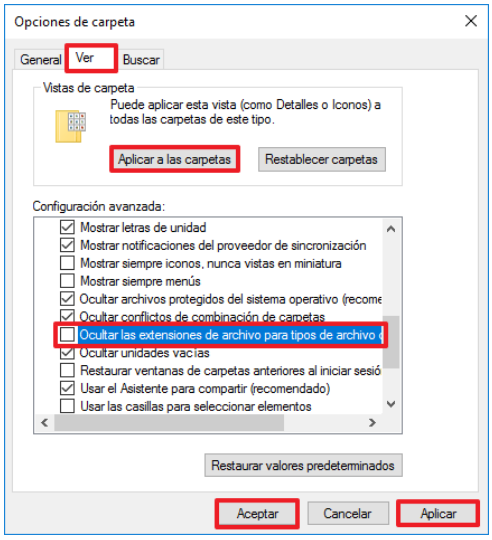
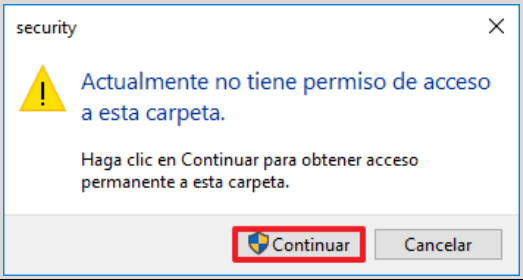
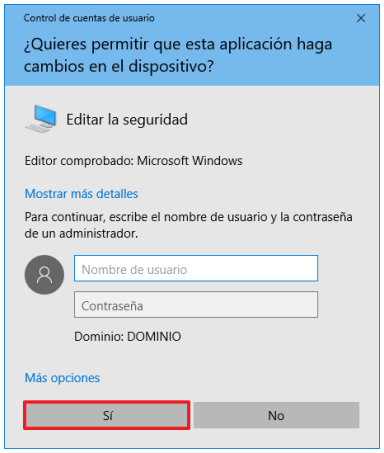


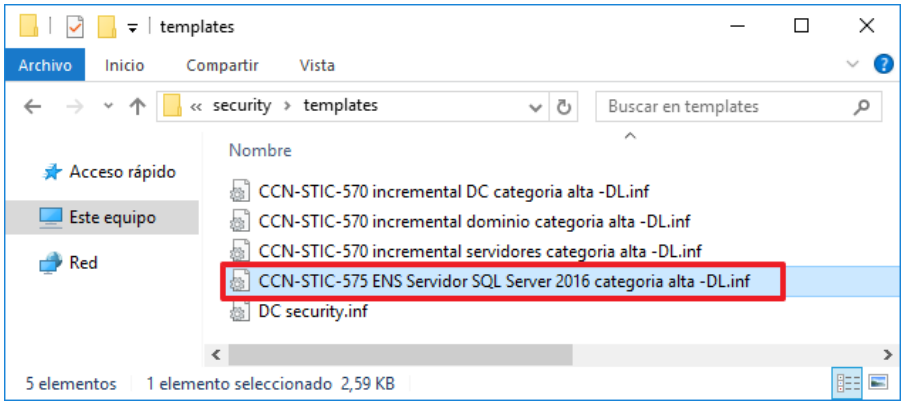
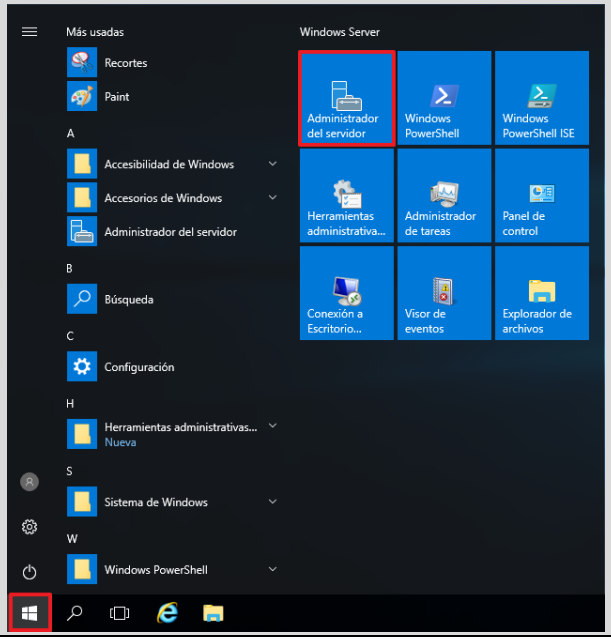
1. PREPARACIÓN DEL DOMINIO

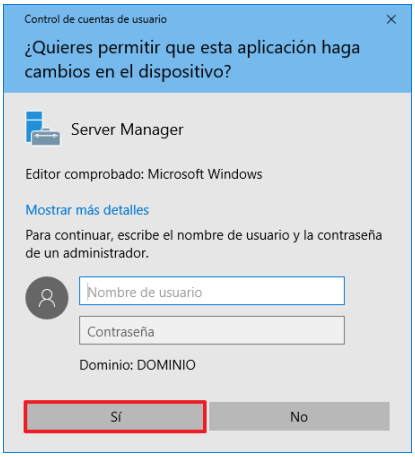
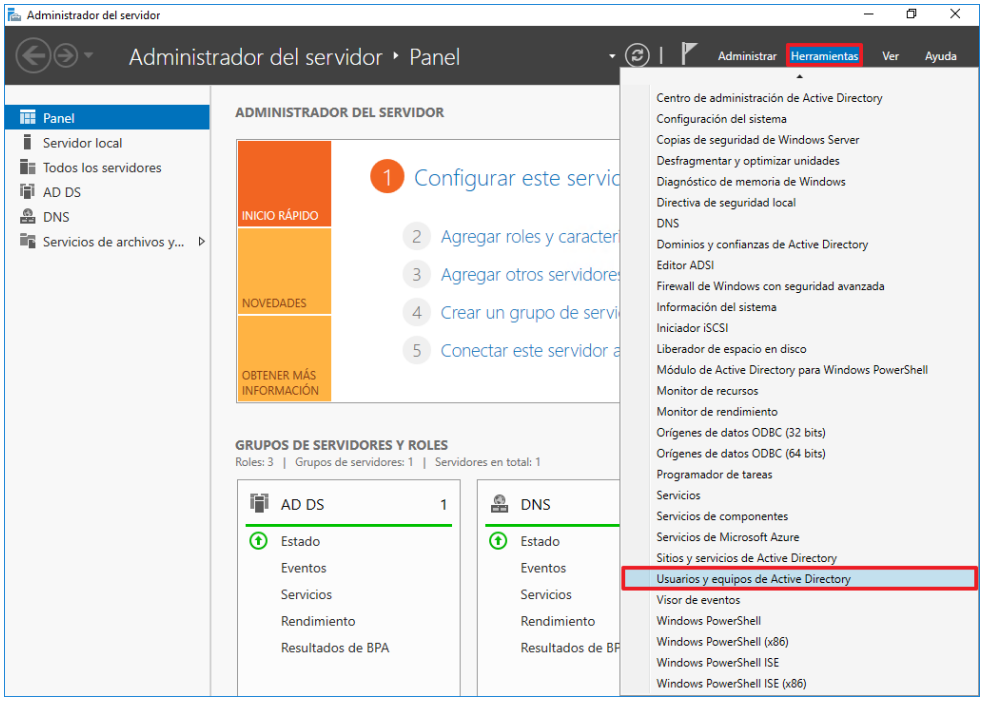
Los pasos que se describen a continuación deberá realizarlos en un Controlador de Dominio del dominio al que pertenece el equipo servidor que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer servidor de SQL Server 2016 que actúe como miembro del dominio. Durante este procedimiento se crea la unidad organizativa que contiene los servidores de SQL Server y se realizan las configuraciones de políticas de grupo correspondientes.

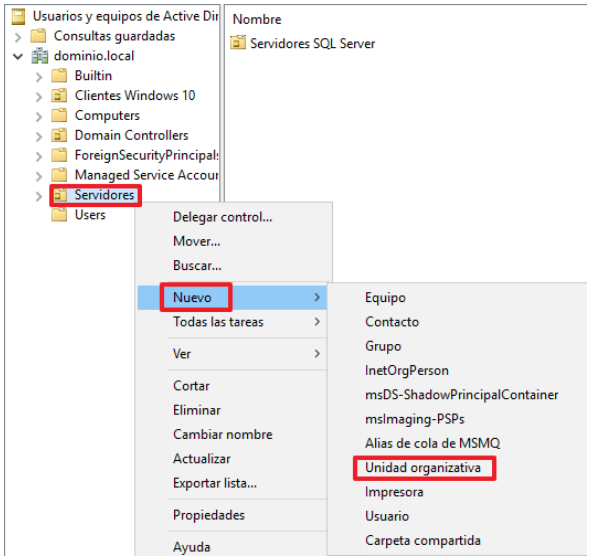
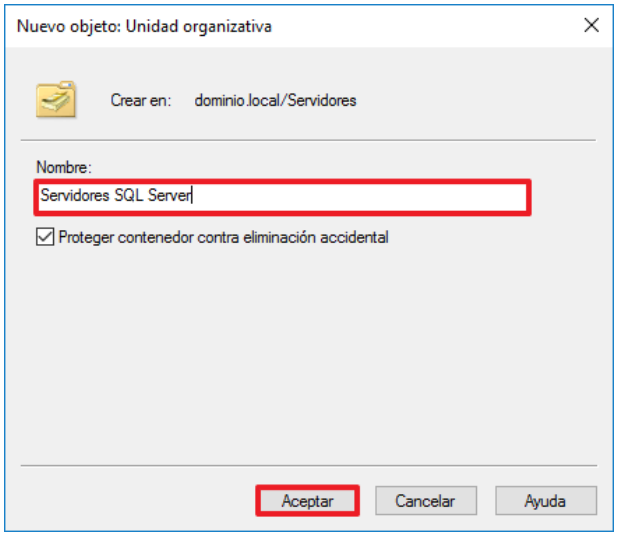
Nota: Esta guía asume que los servidores Controladores del Dominio al que pertenece el Servidor de SQL Server 2016 que está asegurando, se les ha aplicado la configuración descrita en la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016". Si no es así, aplique la guía correspondiente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

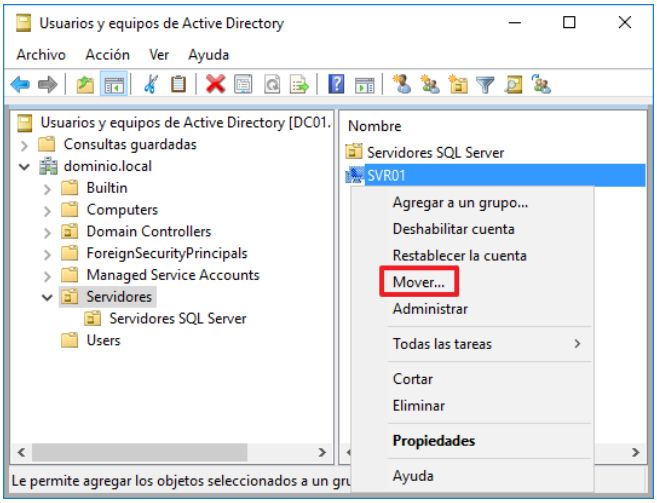
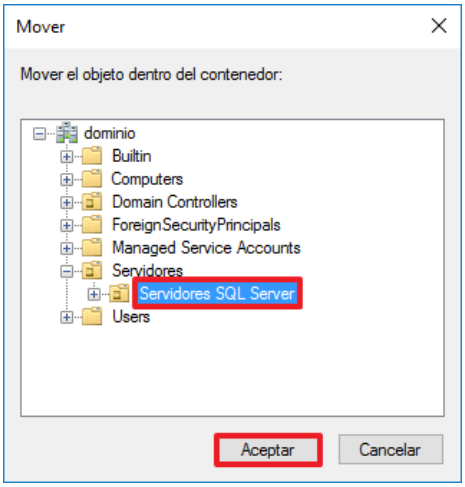
Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio del dominio donde se va a aplicar seguridad para el servidor SQL Server 2016 según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
2.	Cree el directorio "Scripts" en la unidad "C:\". **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.
5.	En el "Explorador de archivos" pulse sobre la pestaña "Vista" del menú superior y seleccione el icono de "Opciones". 

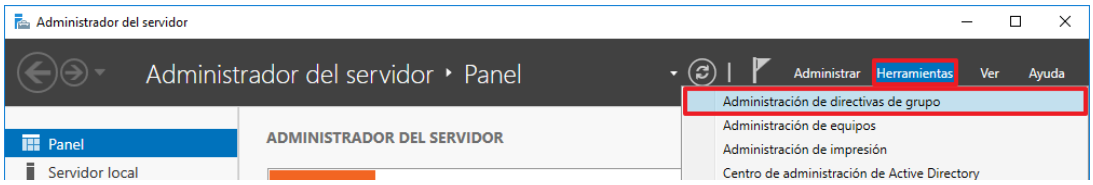
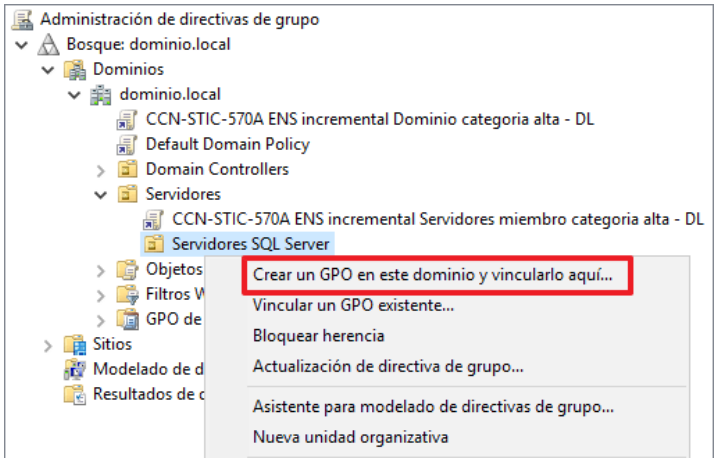
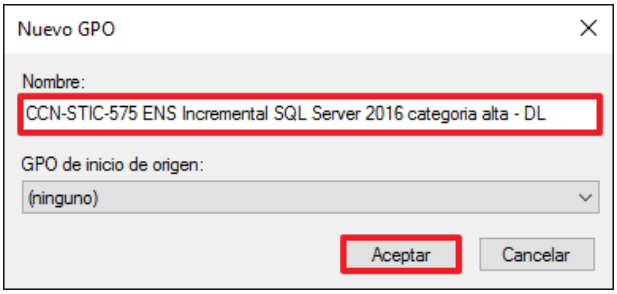
Paso	Descripción
6.	En "Opciones de carpeta" sitúese en la pestaña "Ver" y en el campo "Configuración avanzada" localice y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos". Pulse primero sobre el botón "Aplicar", después sobre "Aplicar a las carpetas" (Pulse "Sí" ante el mensaje de confirmación) y, por último, pulse "Aceptar". 
7.	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. 
8.	El "Control de cuentas de usuarios" le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador de dominio y pulse "Sí". 

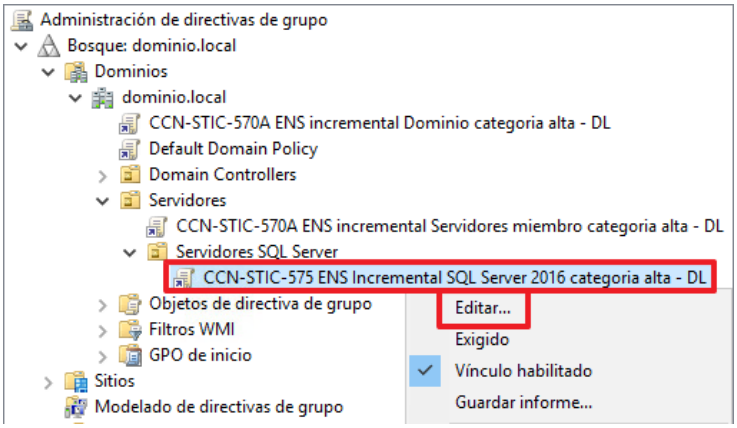
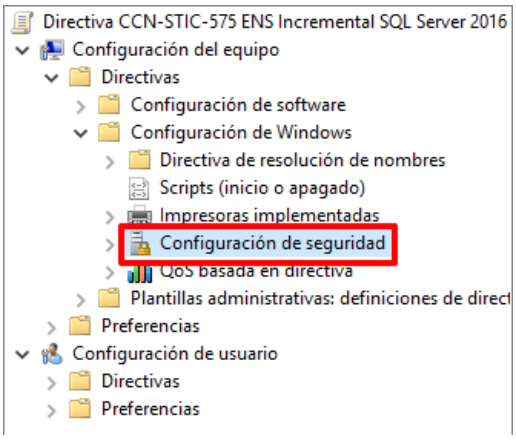
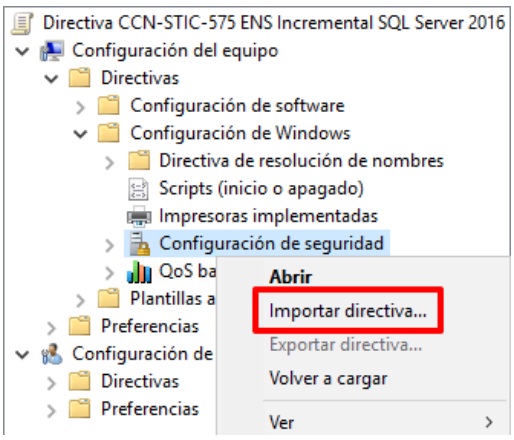
Paso	Descripción
9.	Copie los ficheros "CCN-STIC-575 ENS Servidor SQL Server 2016 categoria alta - DL.inf" al directorio "%SYSTEMROOT%\Security\Templates" del Controlador de Dominio. 
10.	A continuación, abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas.  **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"**. 

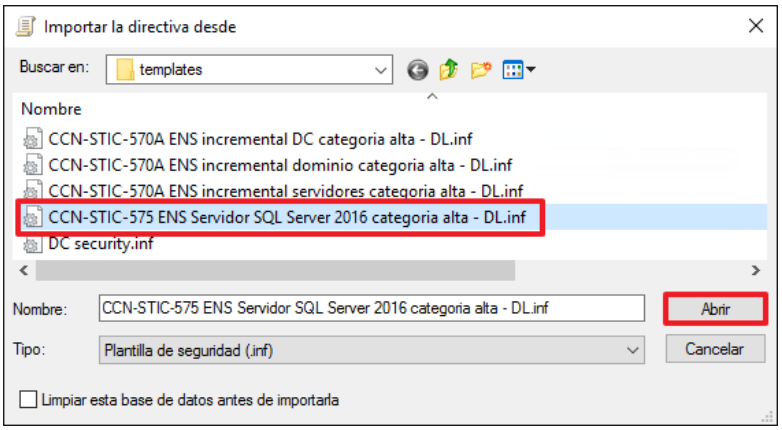
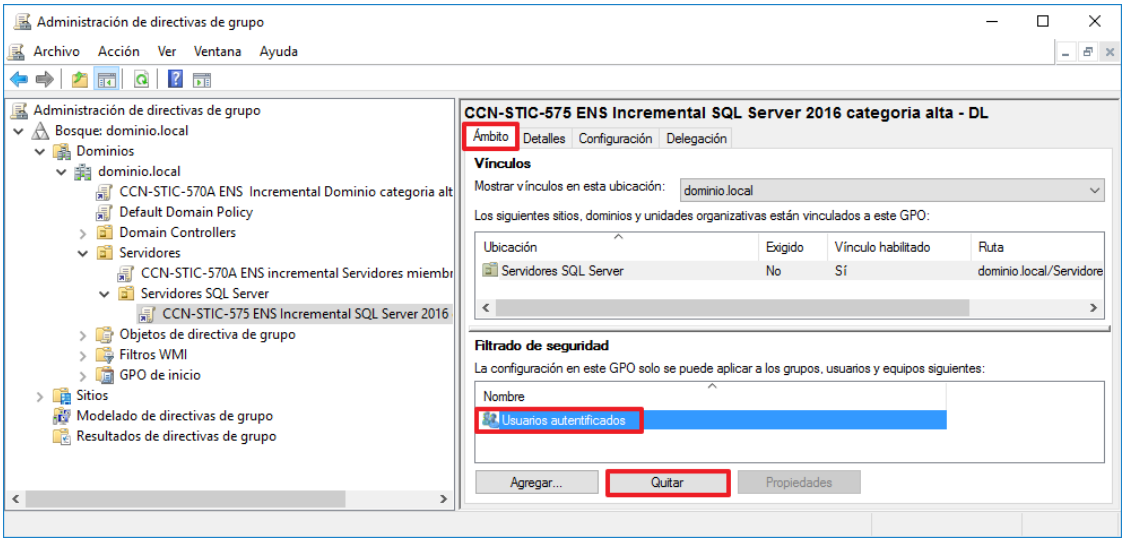
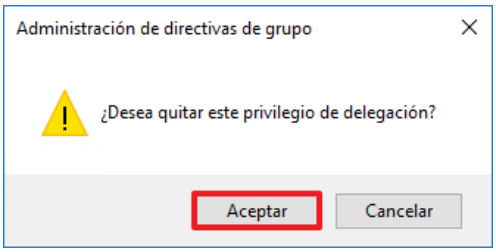
Paso	Descripción
11.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
12.	Inicie la herramienta de usuarios y equipos del Directorio Activo. Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Usuarios y equipos de Active Directory"** 

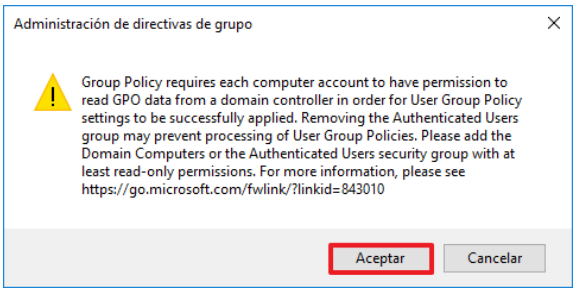
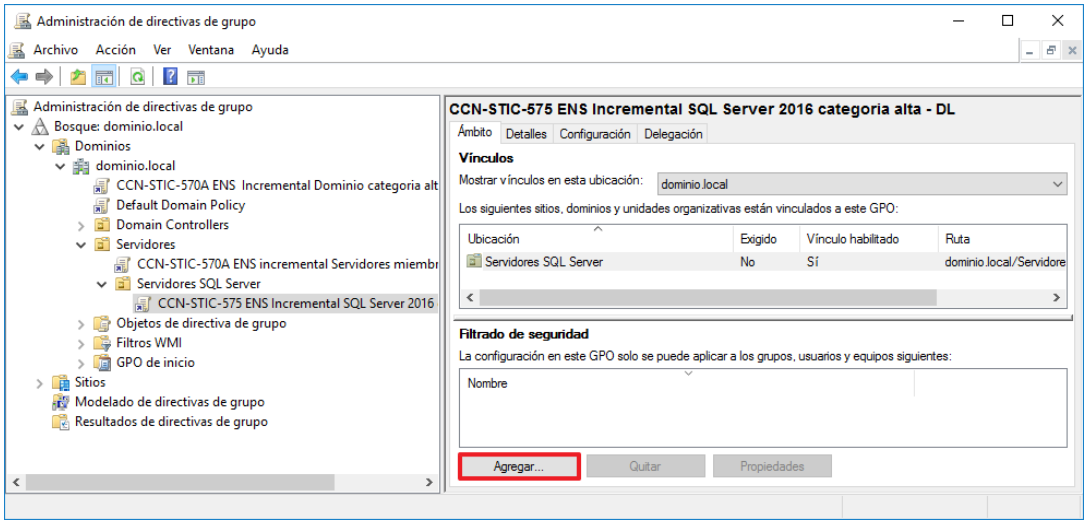
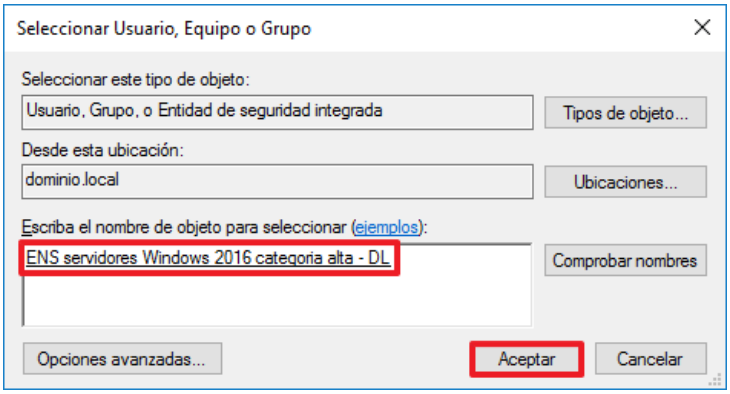
Paso	Descripción
13.	En la consola, cree una nueva unidad organizativa "Servidores SQL Server" dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A Anexo A. Para ello, seleccione el nodo **"<dominio> → <Servidores>"**, y desplegando el menú contextual con el botón derecho, seleccione la opción **"Nuevo → Unidad organizativa".**  **Nota:** En este ejemplo, la unidad organizativa de servidores se encuentra en **"dominio.local/servidores".**
14.	Introduzca el nombre "Servidores SQL Server" tal y como se muestra en la imagen y pulse sobre "Aceptar".  **Nota:** Puede establecer el nombre que más se adecúe a las necesidades de su organización.

Paso	Descripción
15.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores de virtualización a la unidad organizativa "Servidores de SQL Server". Para ello, haga clic con el botón derecho sobre el equipo que desee reubicar y seleccione la opción del menú contextual "Mover...". 
16.	A continuación, seleccione la unidad organizativa "Servidores de SQL Server" y pulse sobre "Aceptar". 
17.	Cierre la herramienta "Usuarios y equipos de Active Directory".
18.	A continuación, deberá crear la GPO "CCN-STIC-575 ENS incremental Servidor de SQL Server categoria alta - DL". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 

Paso	Descripción
19.	Inicie la herramienta "Administración de Directivas de Grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"** 
20.	A continuación, despliegue el nodo **"Bosque: <<nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores SQL Server"**. **Nota:** En este ejemplo el nombre de la unidad organizativa donde se encuentran todos los servidores que implementan este rol, "Servidores SQL Server".
21.	Pulse con el botón derecho sobre la unidad organizativa "Servidores de SQL Server" y seleccione "Crear un GPO en este dominio y vincularlo aquí…". 
22.	Introduzca el nombre del objeto GPO, "CCN-STIC-575 ENS Incremental SQL Server 2016 categoria alta - DL" y haga clic en el botón "Aceptar". 

Paso	Descripción
23.	Seleccione la directiva recién creada "CCN-STIC-575 ENS Incremental SQL Server 2016 categoria alta - DL". Le mostrará una ventana de aviso de la Consola de administración de directivas de grupo, informando que los cambios realizados son globales para la GPO y estos afectarán a todas las ubicaciones en las que se vincule esta GPO. Pulse en "Aceptar" este mensaje y haga clic con el botón derecho sobre ella 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.	Sitúese en la carpeta "%SYSTEMROOT%\Security\Templates" y seleccione el fichero denominado "CCN-STIC-575 ENS Servidor SQL Server 2016 categoria alta - DL.inf", seguidamente pulse 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...".  **Nota:** En caso de no disponer del grupo mostrado, deberá adaptar estos pasos a las necesidades de su organización.
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.

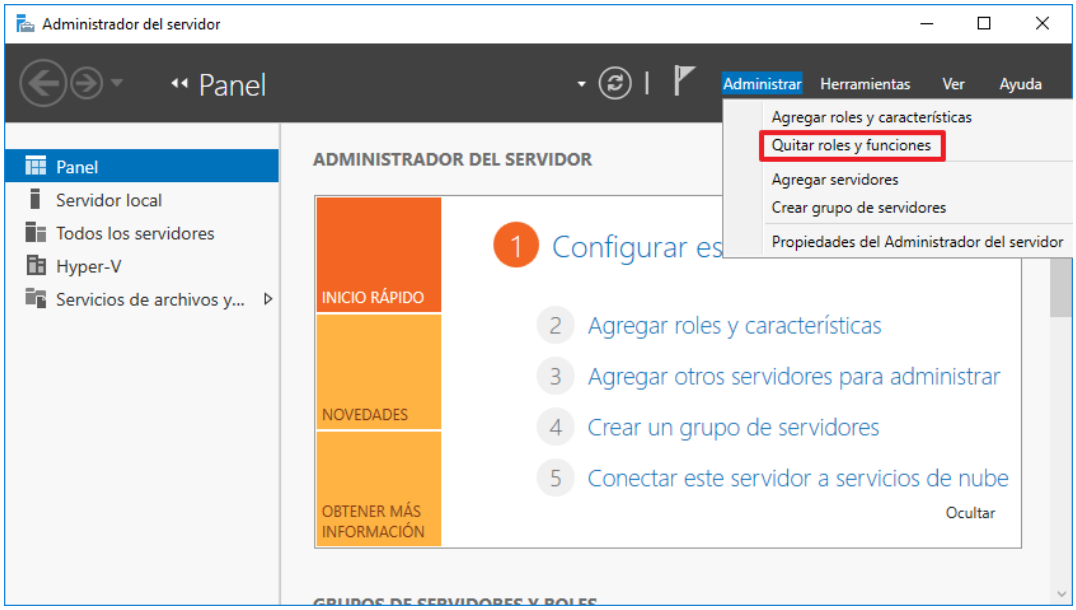
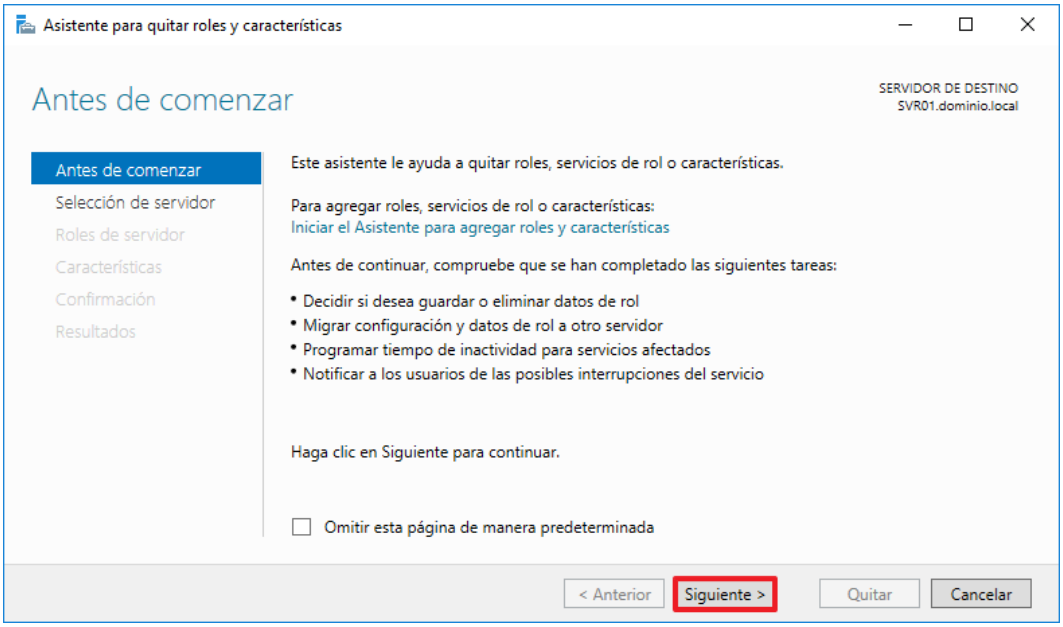
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

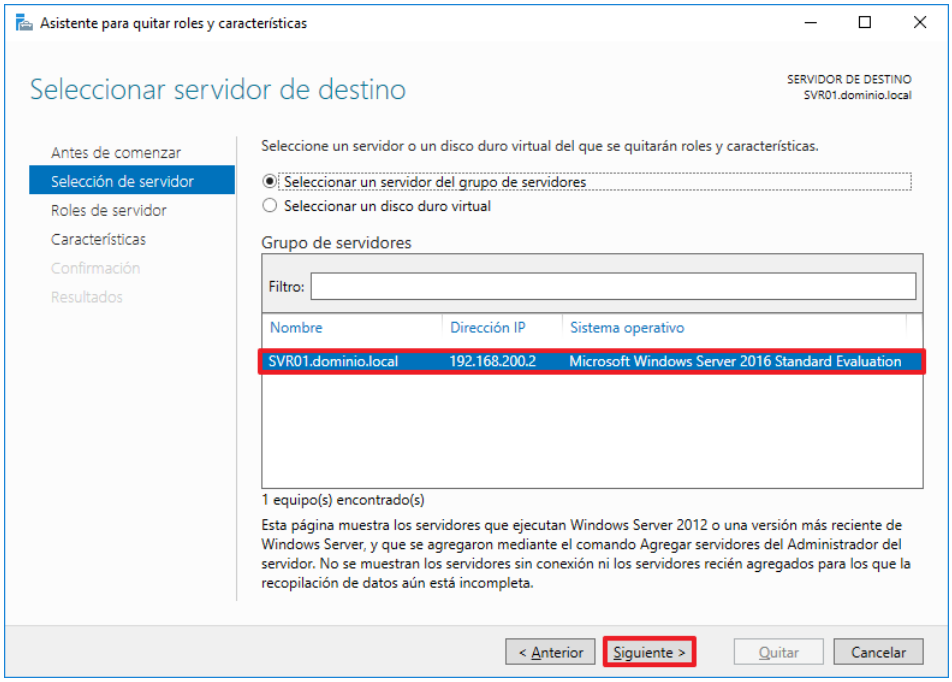
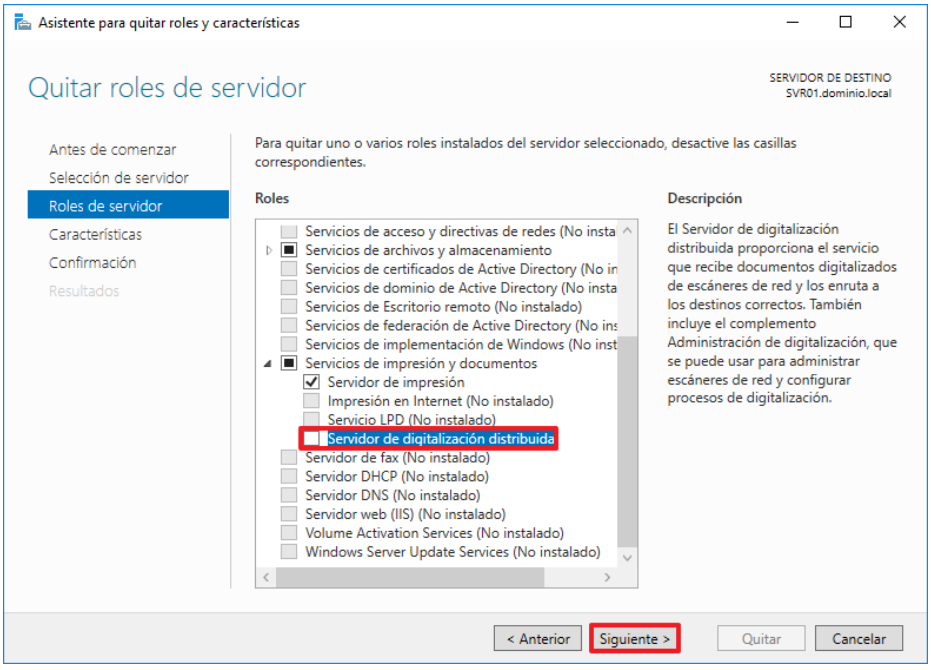
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

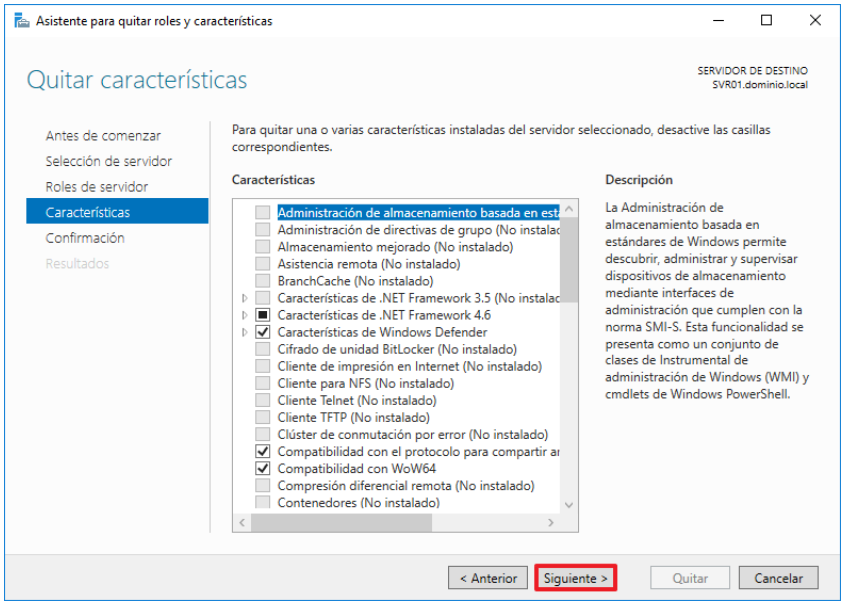
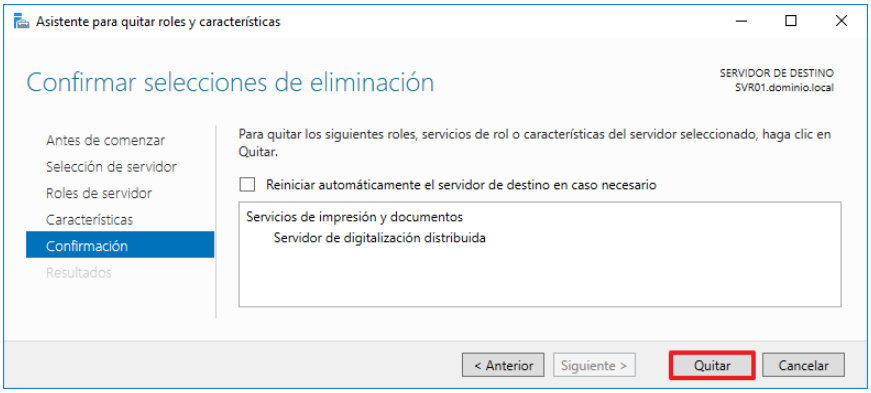
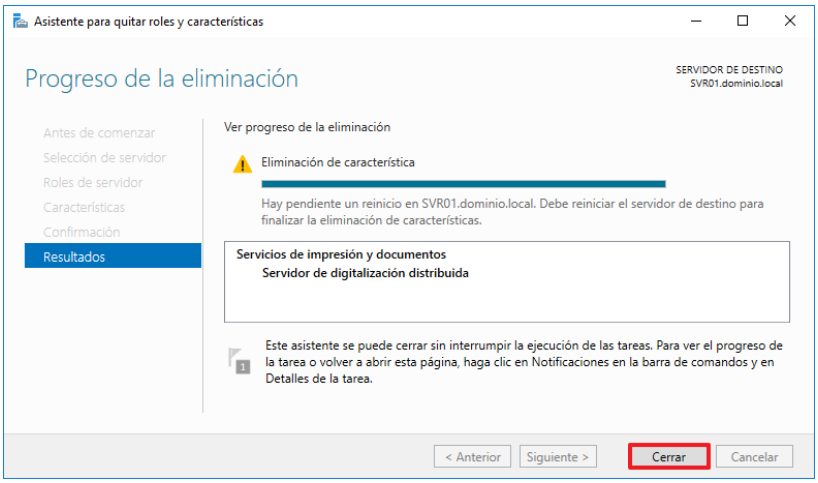
Uno de los aspectos que marca el ENS, desde su requisito de categoría alta - DL en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

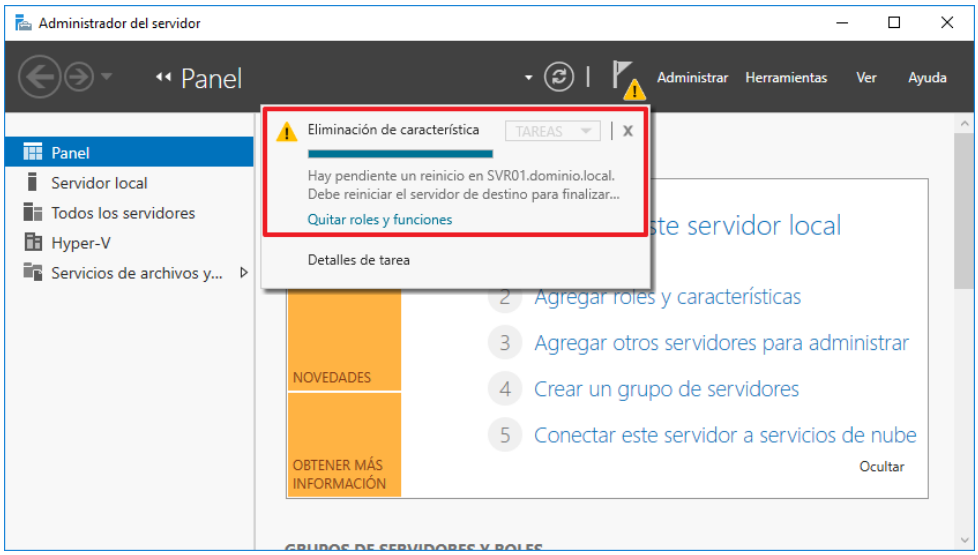
En el procedimiento que se describe a continuación, a modo de ejemplo, desactiva un usuario que actualmente no está siendo utilizado por el Servidor de Base de Datos SQL Server.

Paso	Descripción
33.	Inicie sesión en el equipo miembro del dominio donde se va a aplicar seguridad para el Servidor de SQL Server 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. Introduzca las credenciales de un usuario con permisos de administrador.

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

Paso	Descripción
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. APLICACIÓN DE ESTÁNDARES INTERNACIONALES DE SEGURIDAD

Para que la instalación de SQL Server 2016 cumpla con los estándares internacionales de seguridad, se deben realizar una serie de configuraciones adicionales en el servidor, estas son:

a) Habilitar compatibilidad con dichos estándares de seguridad.

b) Instalar desencadenadores de inicio de sesión.

c) Establecer el proceso de rastreo.

Este procedimiento creará una serie de objetos en la base de datos (tablas, vistas, funciones, triggers y procedimientos almacenados) y un proceso de rastreo que incluye todos los eventos necesarios, junto a la garantía de que este proceso se inicia cada vez que se inicia el servidor. Los objetos creados son los siguientes:

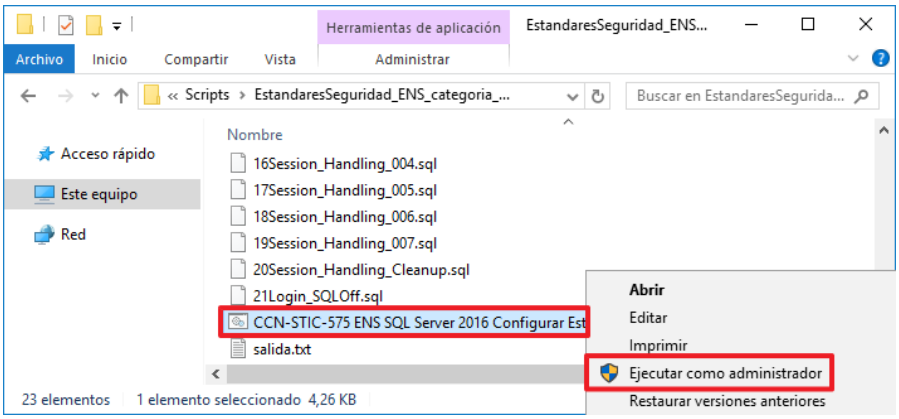
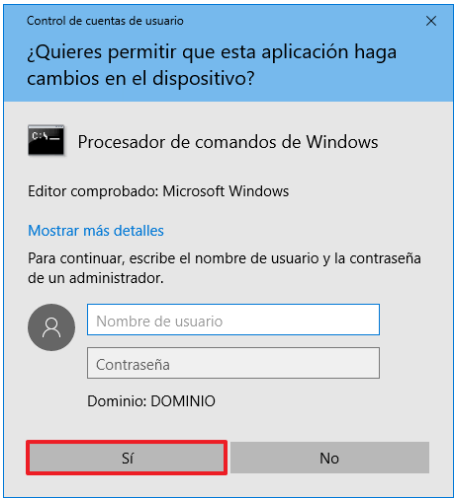
Objeto	Nombre	Descripción
Tabla	denied_logins_A54E382458CA11DB8373B622A1EF5492	Esta tabla contiene los intervalos semanales en la que los inicios de sesión no están autorizados a conectarse a SQL Server. Esta tabla no debe modificarse directamente.
Tabla	maximum_number_of_connections_per_login_A54E382458CA11DB8373B622A1EF5492	Esta tabla contiene el número máximo de conexiones por sesión. Esta tabla no debe modificarse directamente.
Vista	denied_logins	Esta vista vuelca el contenido de la tabla con los intervalos semanales en formato legible por los humanos.

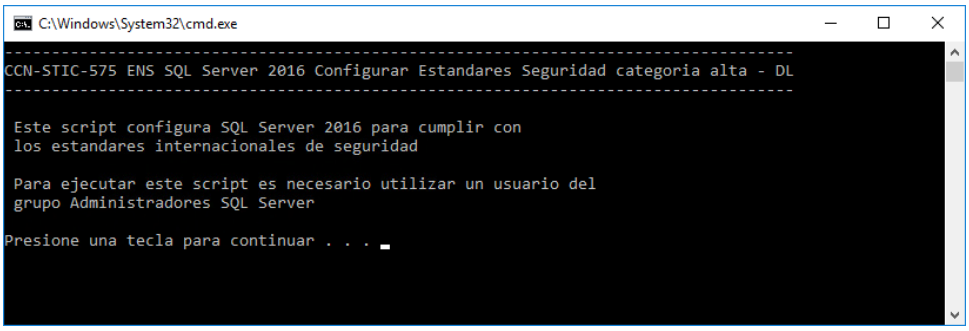
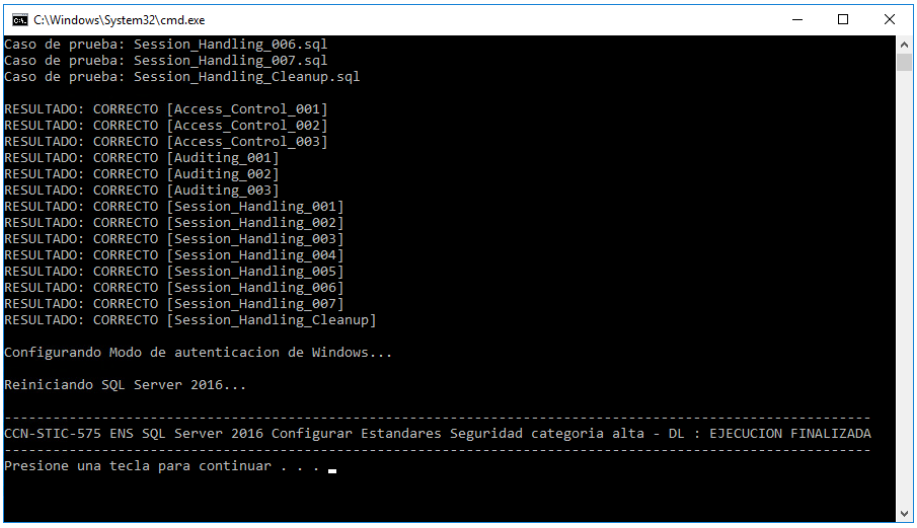
Objeto	Nombre	Descripción
Función	fn_is_original_login_denied_A54E382458CA11DB8373B622A1EF5492	Esta función comprueba si se permite el inicio de sesión original (la que creó la sesión) para iniciar sesión en este momento. El permiso EXECUTE para esta función se concede a todos los usuarios.
Trigger	trig_deny_access_A54E382458CA11DB8373B622A1EF5492	Este trigger se ejecuta en cada intento de inicio de sesión. Comprueba si el login tiene permitido iniciar sesión en ese momento (basado en la hora del día y el día de la semana) y si no se rechaza la conexión lanzando una excepción.
Trigger	trig_max_connections_A54E382458CA11DB8373B622A1EF5492	Este trigger se ejecuta en cada intento de inicio de sesión. Comprueba si el login tiene permitido iniciar sesión en ese momento (basado en el número máximo de sesiones concurrentes por usuario) y si no se rechaza la conexión lanzando una excepción.
Procedimiento almacenado	sp_deny_logon_internal_A54E382458CA11DB8373B622A1EF5492	Procedimiento interno que no debe ejecutarse directamente.
Procedimiento almacenado	sp_deny_logon	Este procedimiento almacenado permite al administrador negar el establecimiento de sesión a un cierto inicio de sesión basado en el día de la semana y la hora del día.
Procedimiento almacenado	sp_revoke_logon_denies	Este procedimiento almacenado permite a un administrador revocar todas las denegaciones de un cierto inicio de sesión.
Procedimiento almacenado	sp_set_maximum_number_of_connections_per_login	Este procedimiento almacenado permite a un administrador establecer el máximo número de conexiones concurrentes permitidas por inicio de sesión.
Procedimiento almacenado	sp_remove_maximum_number_of_connections_limit	Este procedimiento almacenado permite a un administrador eliminar la configuración del máximo número de conexiones concurrentes permitidas por inicio de sesión. Tras la ejecución de este procedimiento almacenado, SQL Server dejará de hacer cumplir cualquier limitación en el número de sesiones concurrentes por inicio de sesión.
Procedimiento almacenado	sp_trace_setcategory	Este procedimiento almacenado permite a un administrador habilitar o deshabilitar una columna de datos específica para todos los eventos en una categoría de traza determinada.
Procedimiento almacenado	sp_trace_setcategory_all	Este procedimiento almacenado permite a un administrador habilitar o deshabilitar todas las columnas de datos válidas para todos los eventos en una categoría de traza determinada.

Como resultado del proceso de rastreo, se generarán una serie de ficheros de traza en la carpeta Log de la carpeta raíz de la instancia SQL Server instalada, donde se registrarán todos los eventos.

Además, durante la ejecución de esta fase se activa la auditoría de inicios de sesión correctos y erróneos.

A continuación, se muestran los pasos necesarios para llevar a cabo esta configuración.

Paso	Descripción
44.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
45.	Localice la carpeta "C:\Scripts\EstandaresSeguridad_ENS_categoria_alta-DL" que previamente se ha copiado al equipo. **Nota:** En caso de no disponer de la carpeta "C:\Scripts" deberán copiar los archivos necesarios en la ruta "C:\Scripts" para continuar con la ejecución del paso a paso.
46.	Ejecute el script "CCN-STIC-575 ENS SQL Server 2016 Configurar Estandares Seguridad categoria alta - DL.bat" con privilegios de administración. Para ello, pulse con el botón derecho "Ejecutar como administrador". 
47.	El control de cuentas de usuario le solicitará las credenciales del usuario del grupo "Administrador SQL Server" que se está utilizando para realizar la configuración. 

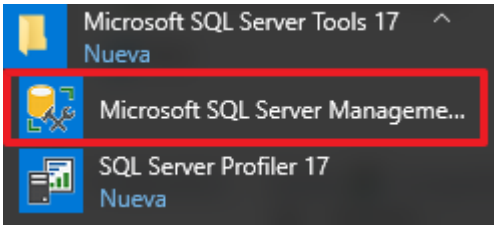
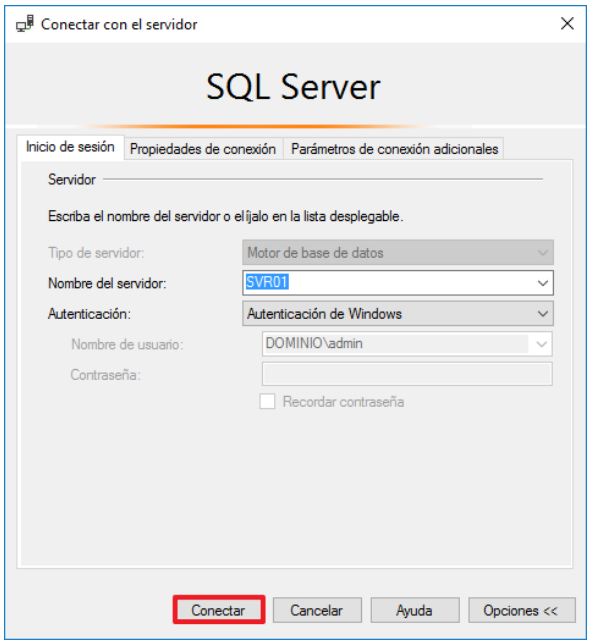
Paso	Descripción
48.	A continuación, aparecerá la siguiente ventana. Presione una tecla para iniciar el proceso. 
49.	Espere a que finalice el proceso. Puede tardar varios minutos en completarse. Una vez finalizada la configuración, presione una tecla para cerrar la ventana.  **Nota:** Omita cualquier advertencia de error que se encuentre fuera del rango de valores "Resultado".
50.	Compruebe que el resultado de todas las pruebas es "CORRECTO". **Nota:** Durante este proceso se activa el modo de autenticación de Windows y SQL para poder llevar a cabo parte de las pruebas. Al finalizar el proceso se vuelve a configurar el Modo de autenticación de Windows.
51.	Pulse una tecla para finalizar la ejecución de la configuración y cerrar la ventana.
52.	Para que el sistema termine de aplicar los cambios deberá reiniciar el servidor donde están aplicando las configuraciones de seguridad.

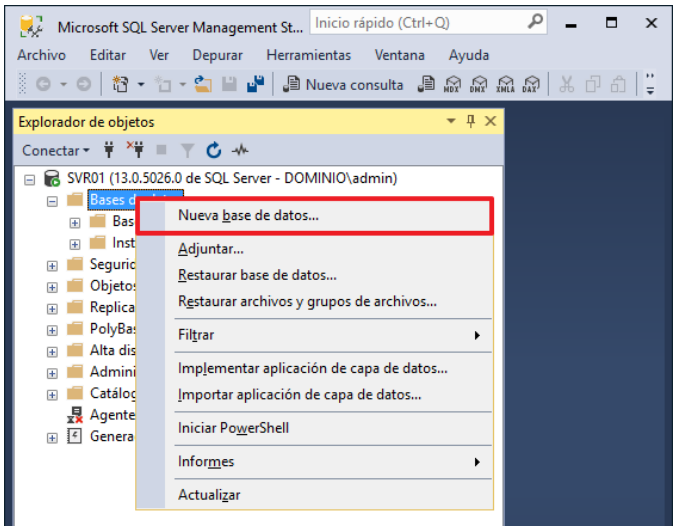
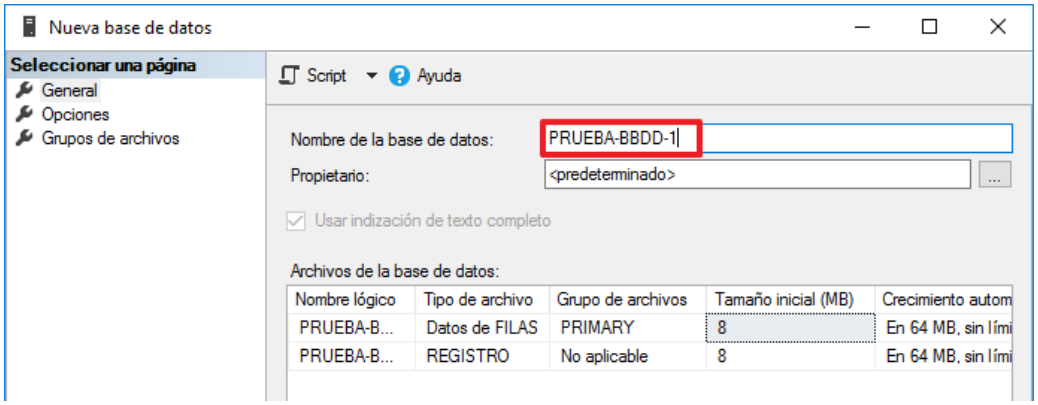
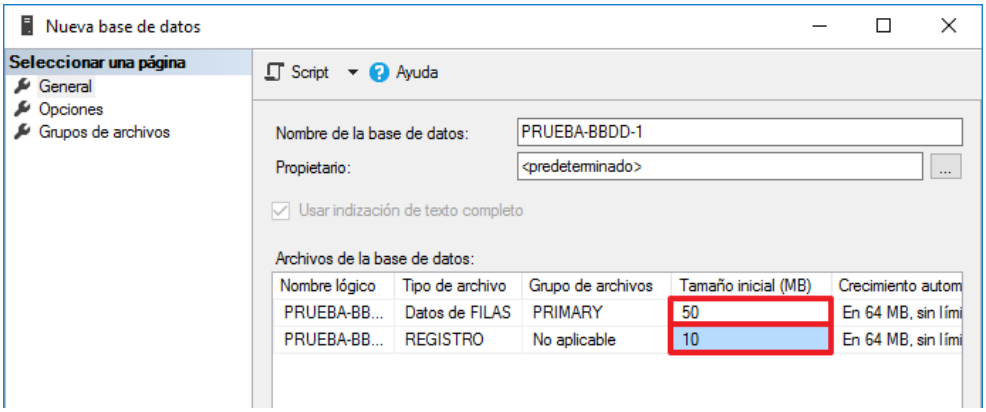
2.3. GESTIÓN DE BASES DE DATOS

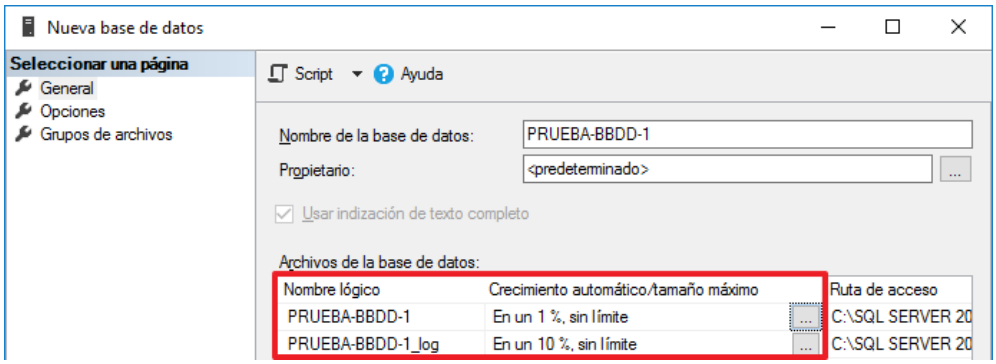
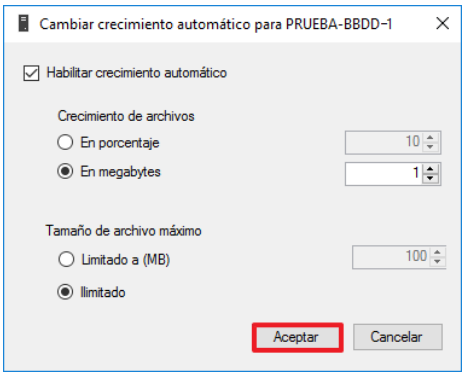
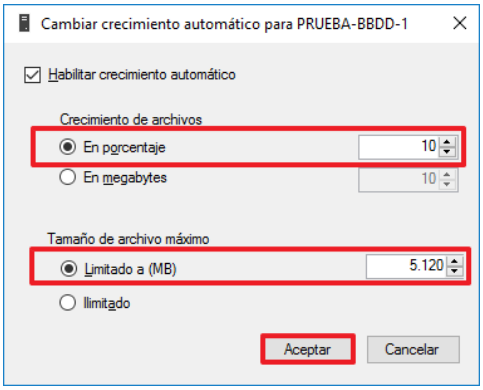
Las bases de datos son el componente sobre el que se apoya SQL Server 2016 para almacenar toda la información que se genera. Este apartado define un ejemplo de cómo gestionar dichas bases de datos.

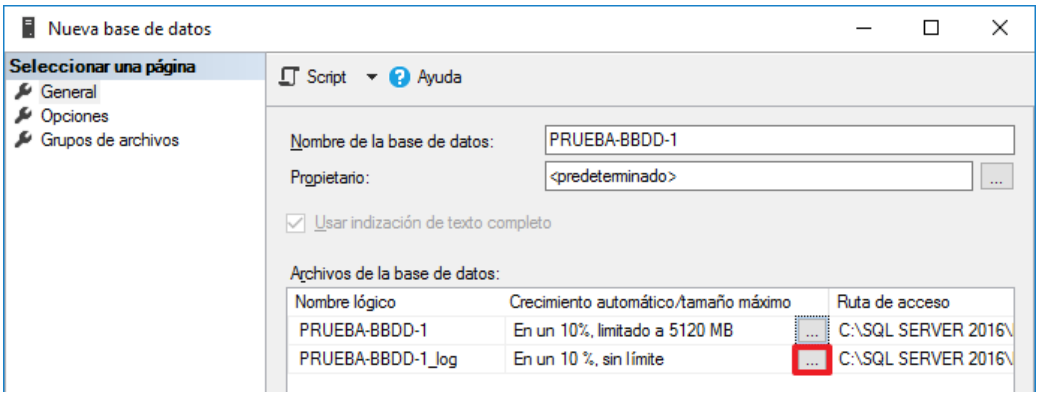
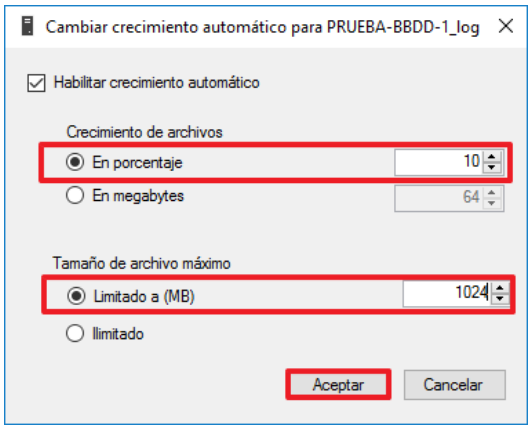
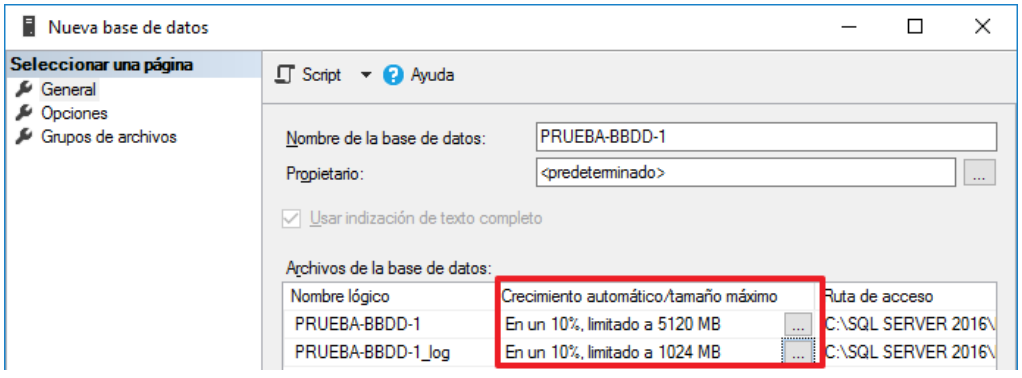
2.3.1. CREACIÓN DE BASES DE DATOS

En esta sección se definen los pasos para crear una nueva base de datos en el servidor SQL.

Paso	Descripción
53.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
54.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
55.	En la ventana de "Conectar con el servidor", es necesario asegurarse que el nombre del servidor es el correcto y pulse "Conectar". 

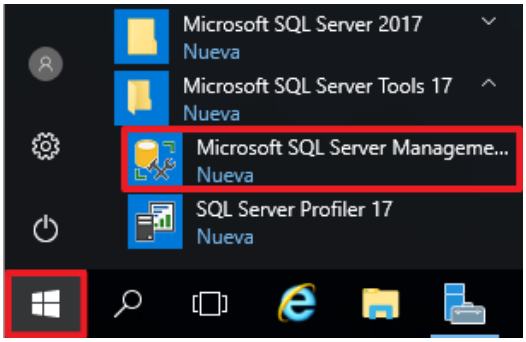
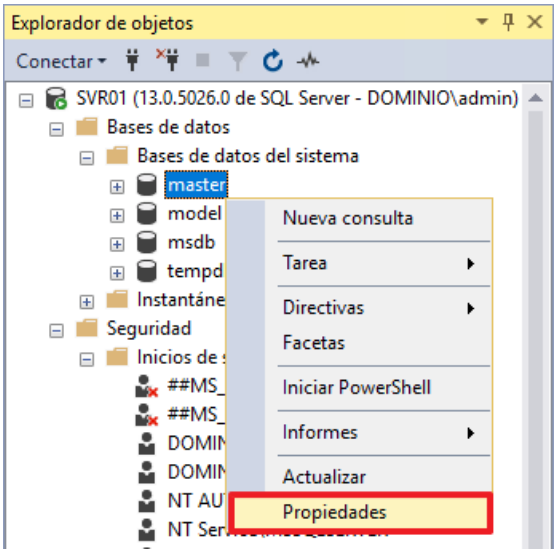
Paso	Descripción
56.	Despliegue el nodo "Bases de datos" y con el botón derecho, seleccione la opción del menú contextual "Nueva base de datos". 
57.	Escriba el nombre de la base de datos que se desea crear.  **Nota:** En este ejemplo se utiliza el nombre "PRUEBA-BBDD-1".
58.	En la zona de archivos de la base de datos, puede especificar el tamaño inicial de la base de datos y el grado de crecimiento automático que se desea aplicar. Por ejemplo, si desea crear una base de datos con 50 MB de tamaño inicial y un fichero de registro de transacciones (log) con 10 MB, entonces establezca los valores 50 y 10 respectivamente. 

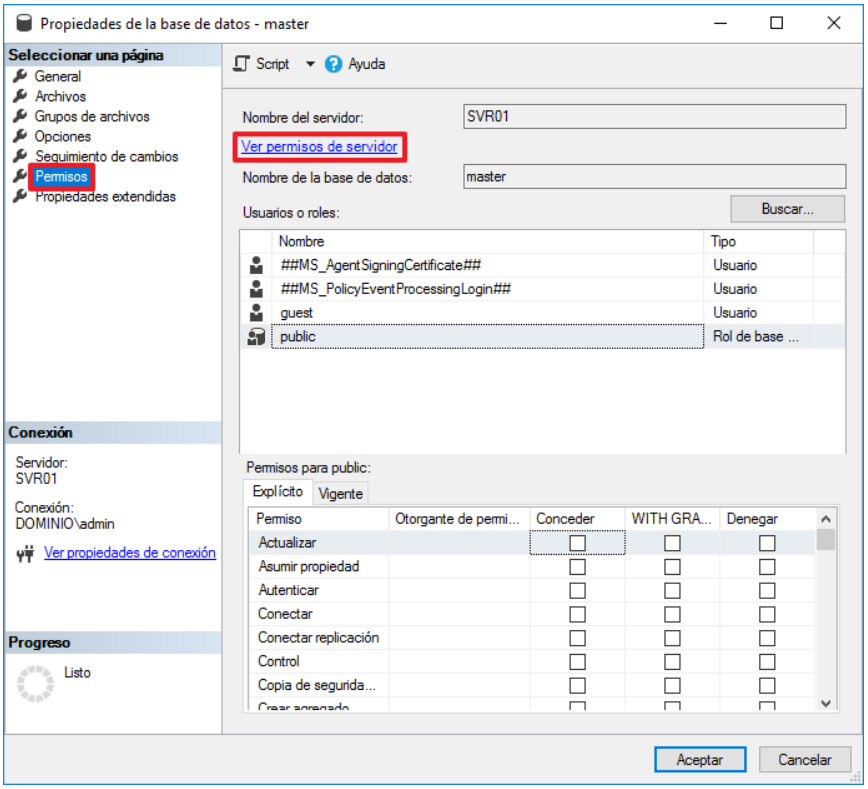
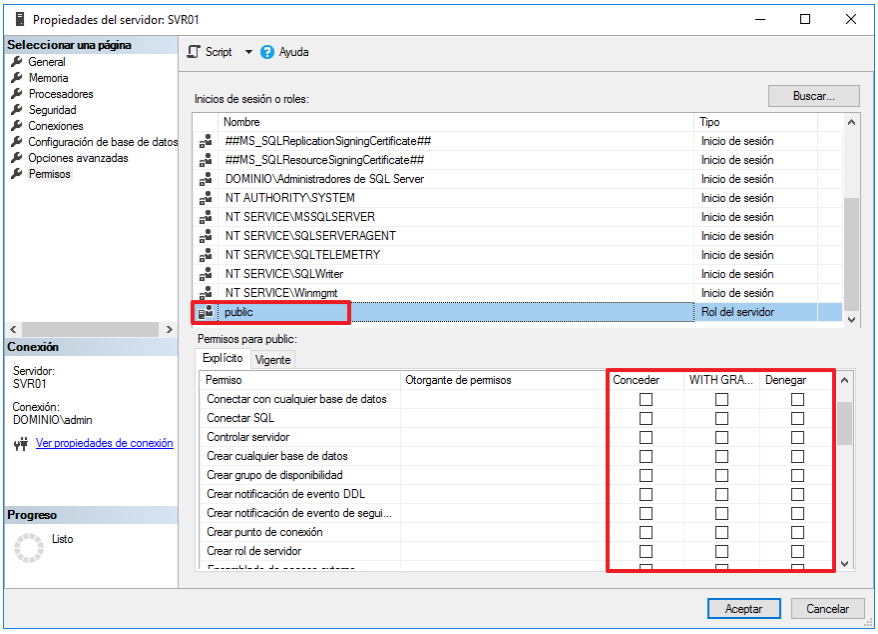
Paso	Descripción
59.	En la columna de crecimiento automático, se establece el grado de crecimiento que se desea implementar para ambos ficheros una vez que se haya alcanzado el tamaño inicial establecido. 
60.	Pulse sobre el primero de los botones "…" para establecer el grado de crecimiento de la base de datos. Pulse "Aceptar" para guardar los cambios.  **Nota:** Puede establecerse el crecimiento en un porcentaje relativo al tamaño de la base de datos o en un valor estático en megabytes (MB). También puede limitarse el crecimiento a un tamaño máximo, para evitar que se pueda consumir todo el espacio del disco físico.
61.	En este ejemplo se va a configurar el crecimiento automático en un porcentaje de 10%, con un límite máximo de 5 GB para la base de datos y 1 GB para el fichero de registro de transacciones.
62.	Seleccione la opción "En porcentaje" y escriba 10. A continuación seleccione la opción "Limitar el crecimiento de los archivos (MB)" y escriba 5120. Pulse sobre el botón "Aceptar". 

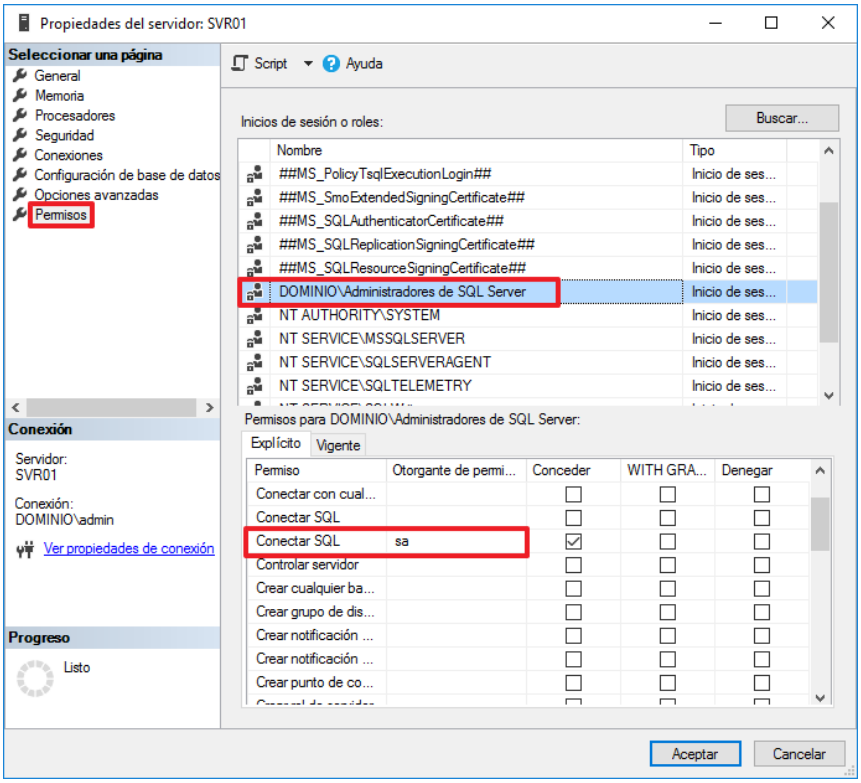
Paso	Descripción
63.	Pulse sobre el segundo de los botones "…" para establecer el grado de crecimiento del fichero de registro de transacciones de la base de datos. 
64.	Debe seleccionarse la opción "En porcentaje" y escriba 10. A continuación seleccione la opción "Limitado a (MB)" y escriba 1024. Pulse sobre el botón "Aceptar". 
65.	Compruebe que los valores introducidos son correctos. 

2.3.2. MODIFICACIÓN DE BASES DE DATOS

En esta sección se definen los pasos para modificar parámetros de seguridad de una base de datos en el servidor SQL.

Paso	Descripción
66.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
67.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
68.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".
69.	En la consola "SQL Server Management Studio", seleccione la carpeta "Bases de datos" y diríjase a aquella base de datos que quiera modificar dentro de "Bases de datos del sistema".  **Nota:** En este ejemplo, se modificará la base de datos "master".

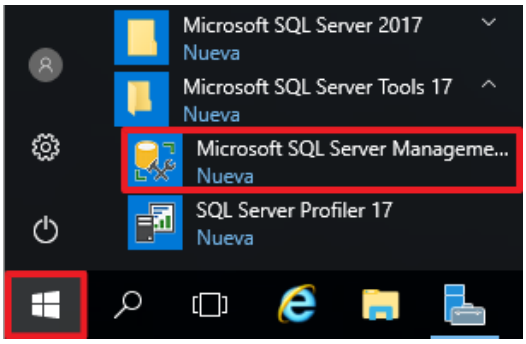
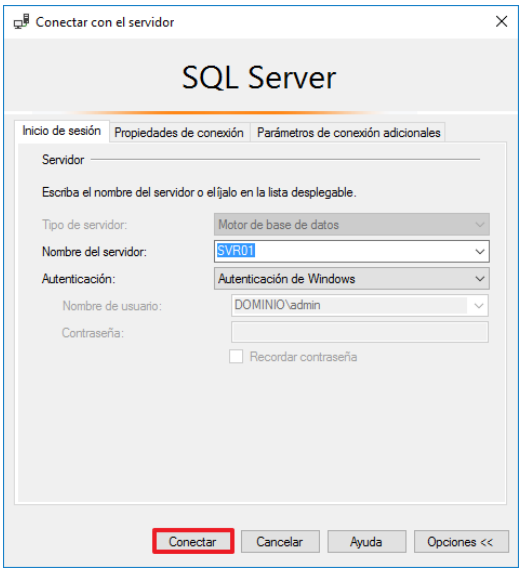
Paso	Descripción
70.	Seleccione la pestaña "Permisos" del panel izquierdo y finalmente pulse la opción "Ver permisos del servidor". 
71.	En esta pantalla puede cambiar los permisos de cada inicio de sesión y/o rol del servidor. marcando los distintos inicios de sesión en el panel superior se muestran los permisos de éste. 

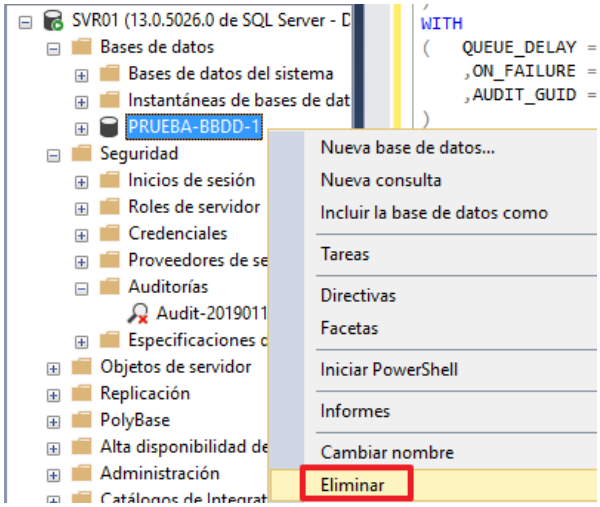
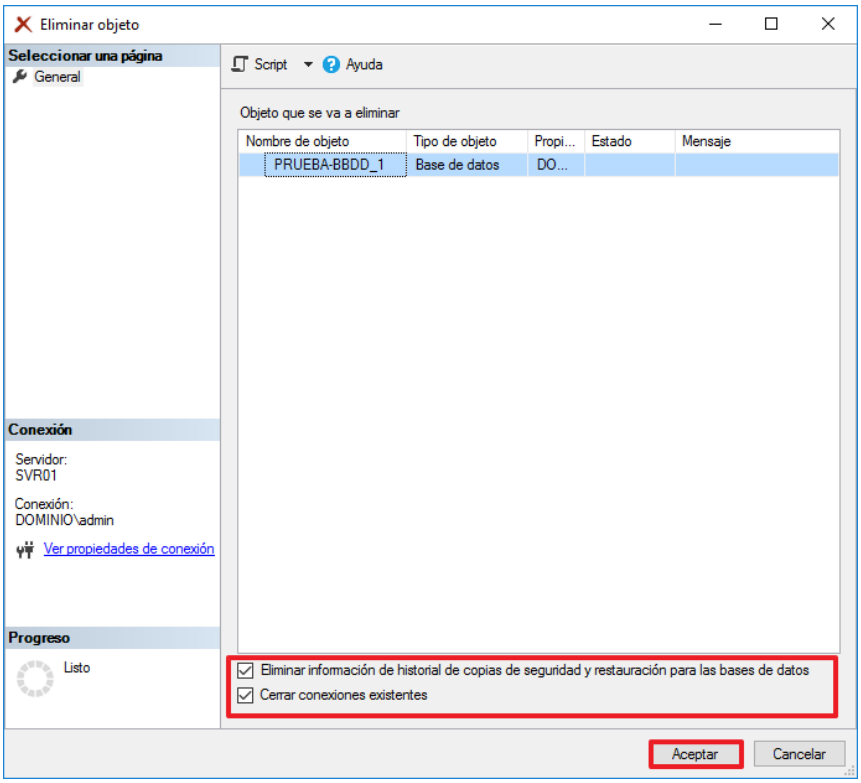
Paso	Descripción
72.	Es necesario asegurarse que después de haber dado de alta todos los inicios de sesión necesarios de su organicación tan sólo un inicio de sesión o rol puede cambiar los permisos del resto de usuarios tal y como se ve en la siguiente pantalla.  **Nota:** Para más información sobre los servicios de servidores asociados a las cuentas de SQL Server puede consultar la página https://docs.microsoft.com/es-es/sql/database-engine/configure-windows/configure-windows-service-accounts-and-permissions?view=sql-server-2016.

2.3.3. ELIMINACIÓN DE BASES DE DATOS

A continuación, se describe el proceso de eliminación de una base de datos a modo de ejemplo.

Paso	Descripción
73.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.

Paso	Descripción
74.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
75.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar". 

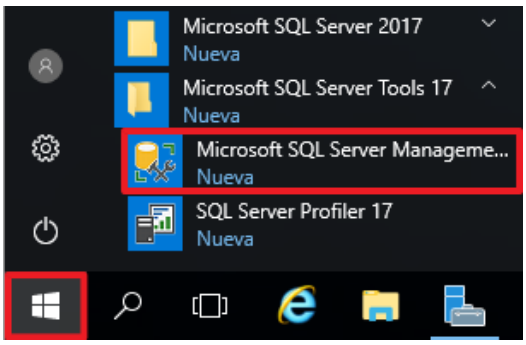
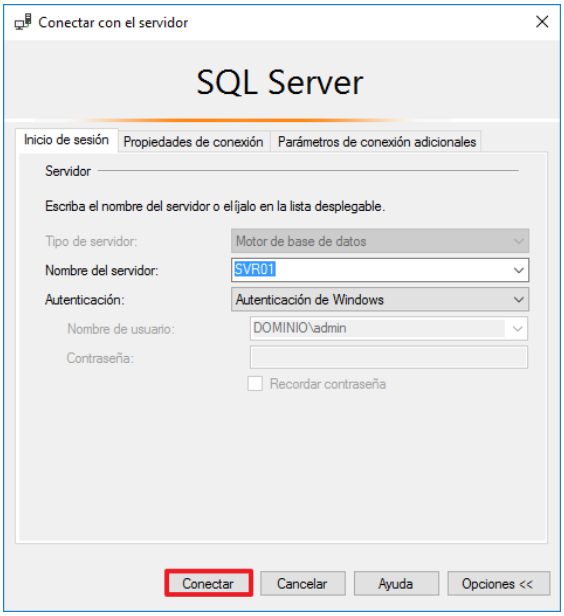
Paso	Descripción
76.	Sitúese en el nodo del árbol "Bases de datos" y seleccione la base de datos que quiera eliminar. Haga clic derecho sobre ella y pulse "Eliminar".  **Nota:** En este ejemplo se procede a eliminar la base de datos llamada "PRUEBA-BBDD-1".
77.	En la siguiente pantalla, marque las opciones "Eliminar información de historial de copias de seguridad y restauración para las bases de datos" y "Cerrar conexiones existentes", finalmente pulse "Aceptar" para eliminar la base de datos. 

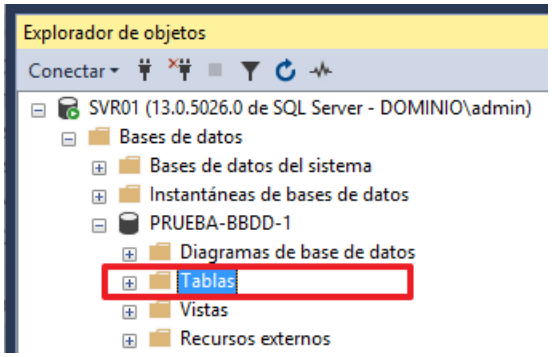
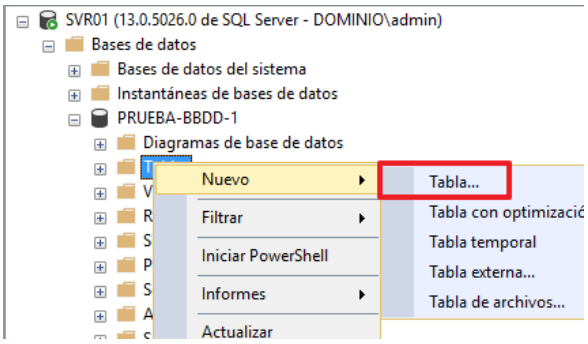
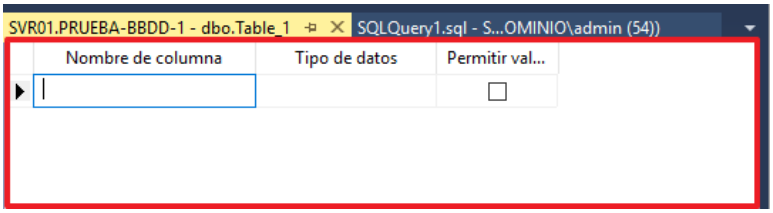
2.4. GESTIÓN DE TABLAS

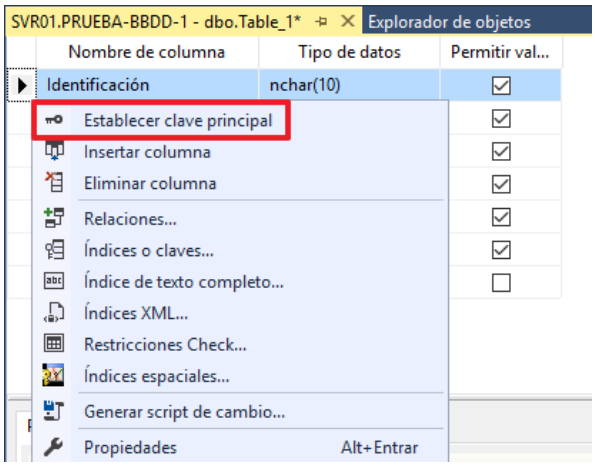
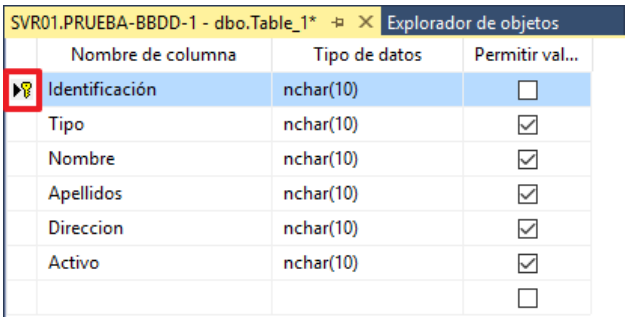
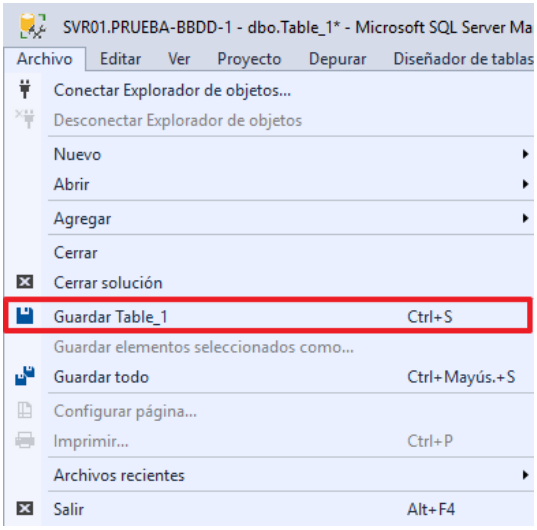
La gestión de tablas dentro de SQL Server 2016 constituye una importante tarea de administración debido a que permite establecer o modificar configuraciones que afectan a la funcionalidad del servicio de base de datos.

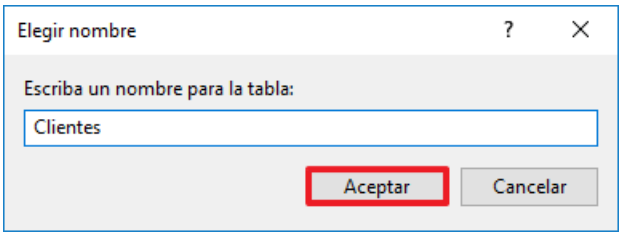
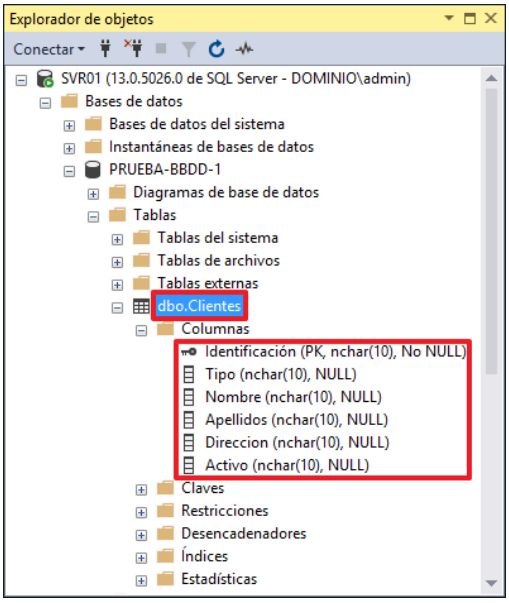
2.4.1. CREACIÓN DE TABLAS

En este apartado se definen los pasos para crear una nueva base de datos en el servidor SQL.

Paso	Descripción
78.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
79.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".** 
80.	En la ventana de "Conectar con el servidor", asegúrese de que el nombre del servidor es el correcto y pulse "Conectar". 

Paso	Descripción
81.	En la consola "SQL Server Management Studio", sitúese en la base de datos donde desee crear una nueva tabla y diríjase a la carpeta "Tablas". la carpeta "Tablas" de la base de datos "PRUEBA-BBDD-1" creada anteriormente, tal y como se observa en la imagen.  **NOTA:** En este ejemplo, se procede a crear una tabla dentro de la base de datos "PRUEBA-BBDD-1".
82.	Con el botón derecho sobre "Tablas", seleccione la opción del menú contextual **"Nuevo → Tabla…".** 
83.	En el área "Nombre de columna", establezca un nombre a cada una de las columnas que va a tener la nueva tabla, así como el tipo de dato correspondiente.  **Nota:** Se recomienda no incluir caracteres especiales en los nombres de las columnas, tales como tildes, signos de exclamación, interrogación o cedillas.

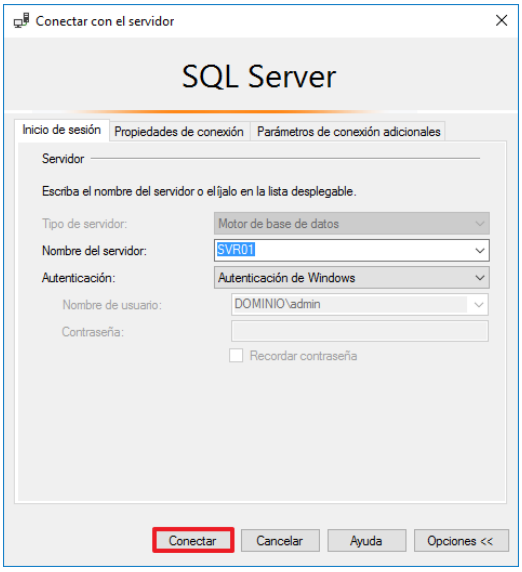
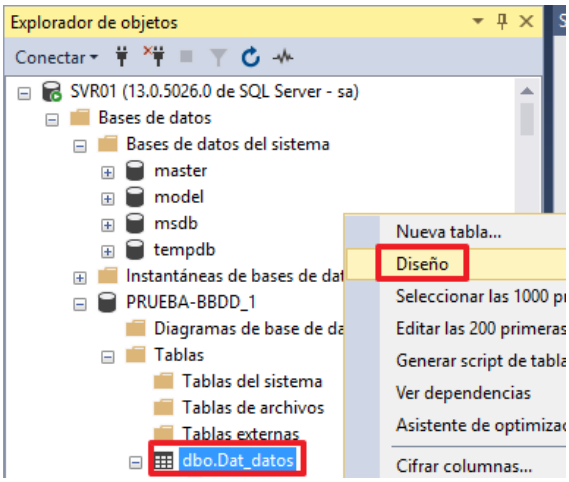
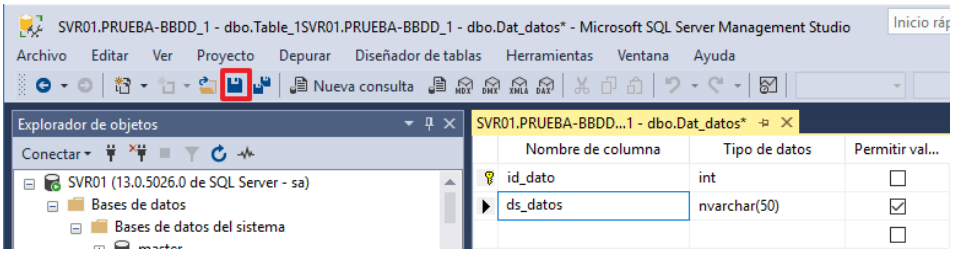
Paso	Descripción
84.	Cuando haya finalizado de introducir las diferentes columnas, será necesario establecer una clave principal dentro de la nueva tabla. Para ello, seleccione aquella columna que desea establecer como llave primaria y pulsando con el botón derecho sobre ella, seleccione la opción del menú contextual "Establecer clave primaria".  **Nota:** En este ejemplo, se utiliza la columna "Identificación".
85.	Asegúrese que aparece una llave sobre la columna que ha establecido como clave primaria como se muestra en la siguiente imagen. 
86.	Para guardar los cambios realizados, pulse sobre la opción del menú contextual **"Archivo → Guardar Table_1".** 

Paso	Descripción
87.	Establezca un nombre para la nueva tabla acorde a las necesidades de su organización y pulse sobre el botón "Aceptar".  **Nota:** En este ejemplo, se utiliza el nombre "Clientes".
88.	Ahora, en el Explorador de objetos, acceda a la nueva tabla para obervar las columnas creadas en pasos anteriores. 

2.4.2. MODIFICACIÓN DE TABLAS

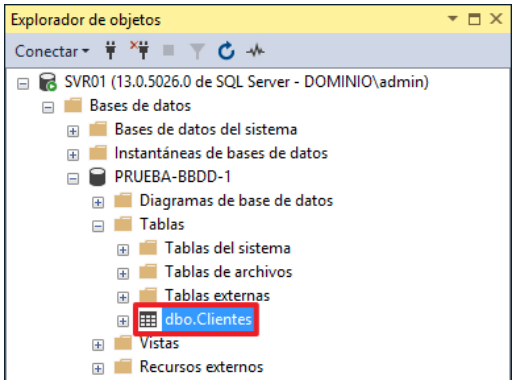
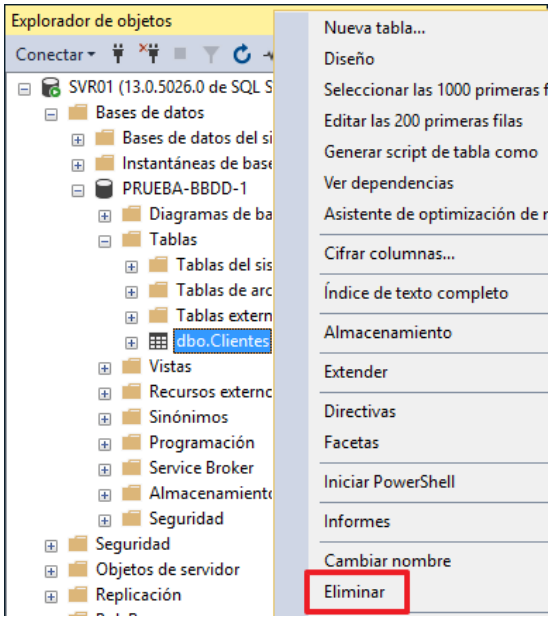
Puede modificarse una tabla desde SSMS (SQL Server Management Studio), a continuación, se describe el procedimiento para modificar una tabla.

Paso	Descripción
89.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
90.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**.

Paso	Descripción
91.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar". 
92.	En la consola "SQL Server Management Studio" localice la tabla que desea modificar, y pulsando con el botón derecho sobre ella, seleccione la opción del menú contextual "Diseño". 
93.	Ahora, podrá realizar los cambios que considere oportunos para su organización. Para guardar los cambios, pulse el botón "guardar". 

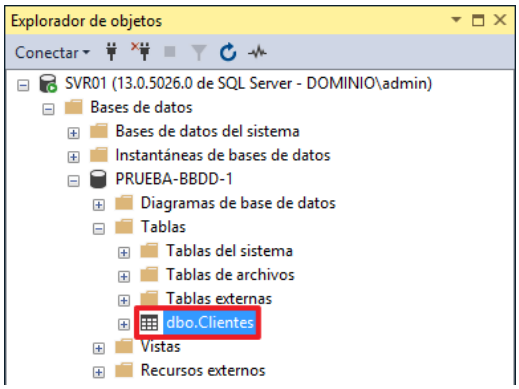
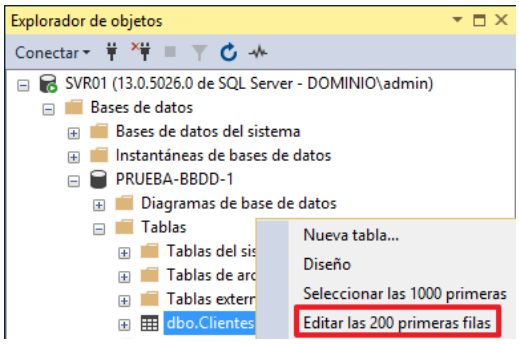
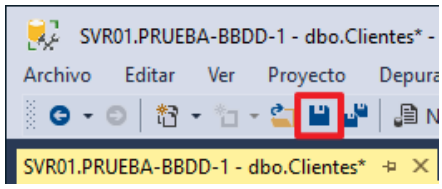
2.4.3. ELIMINACIÓN DE TABLAS

En este punto se describe el procedimiento de eliminación de una tabla a modo de ejemplo.

Paso	Descripción
94.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
95.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".**
96.	En la ventana de "Conectar con el servidor", asegúrese de que el nombre del servidor es el correcto y pulse "Conectar".
97.	Dentro del Explorador de objetos, expanda el árbol "Bases de datos" hasta llegar a la tabla que desea eliminar.  **Nota:** En este ejemplo, se utiliza la tabla "dbo.Clientes".
98.	Una vez seleccionada la tabla, haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Eliminar". 

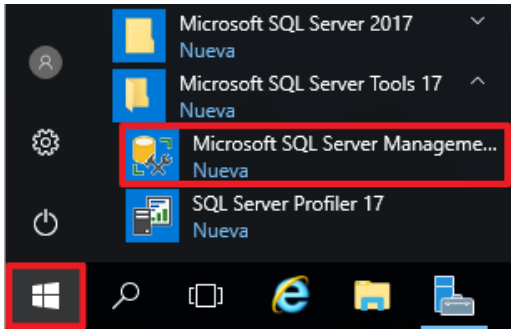
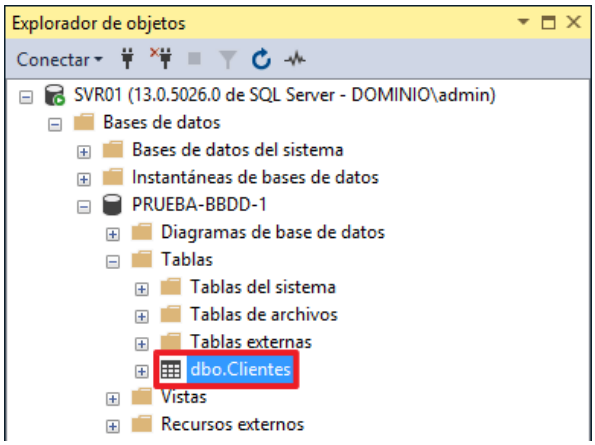
2.4.4. INSERCIÓN DE DATOS

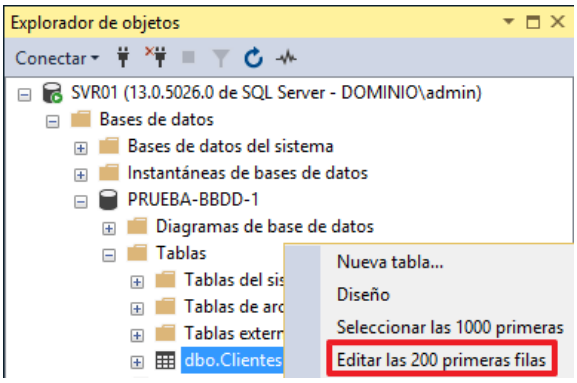
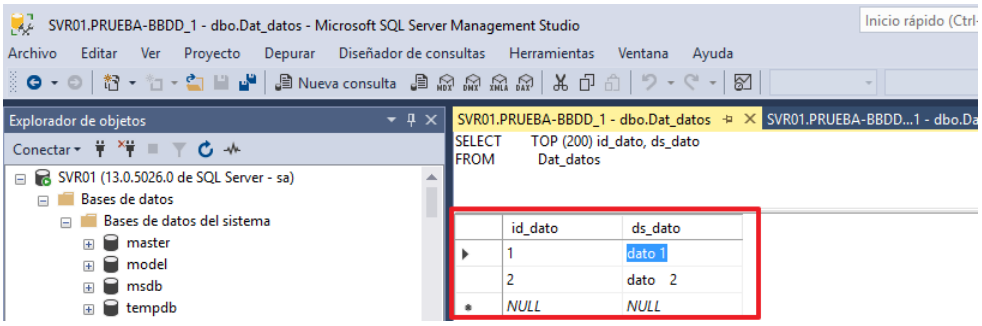
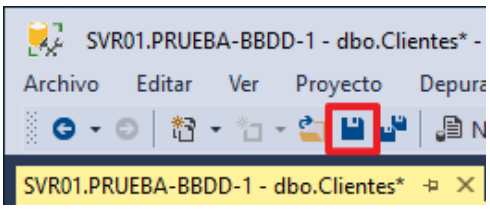
En este procedimiento se muestra a modo de ejemplo el método de inserción de datos.

Paso	Descripción
99.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
100.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**.
101.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".
102.	Dentro del Explorador de objetos, expanda el árbol "Bases de datos" hasta llegar a la tabla que desea insertar datos.  **Nota:** En este ejemplo, se utiliza la tabla "dbo.Clientes".
103.	Una vez seleccionada la tabla, haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Editar las 200 primeras filas" para insertar los datos en la tabla seleccionada. 
104.	Una vez finalizada la inserción de datos, pulse el botón "Guardar" para salvaguardar los datos introducidos. 

2.4.5. MODIFICACIÓN DE DATOS

En este procedimiento se muestra, a modo de ejemplo, el método para modificar datos de una tabla.

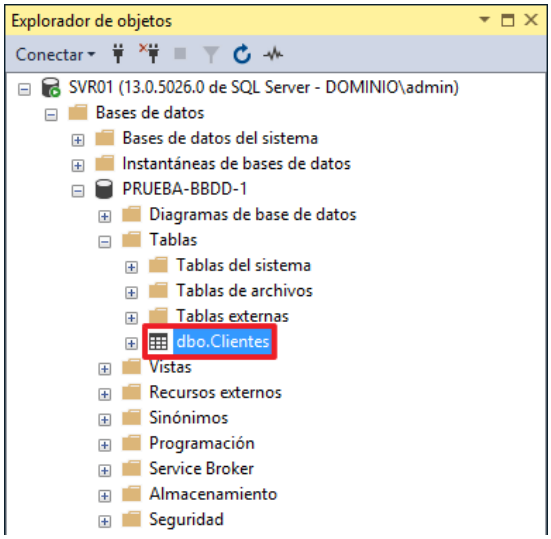
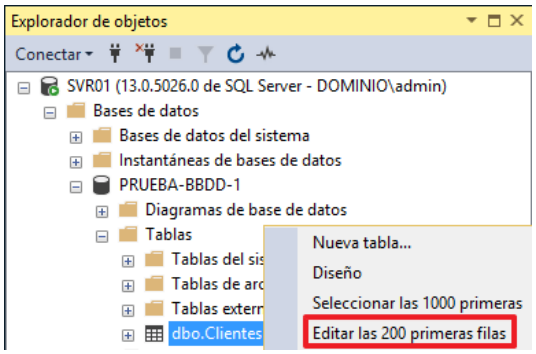
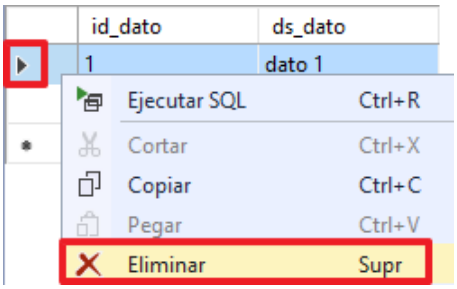
Paso	Descripción
105.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
106.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
107.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse Conectar".
108.	Dentro del Explorador de objetos, expanda el árbol "Bases de datos" hasta llegar a la tabla que desea insertar datos.  **Nota:** En este ejemplo, se utiliza la tabla "dbo.Clientes".

Paso	Descripción
109.	Una vez seleccionada la tabla, haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Editar las 200 primeras filas". 
110.	En la siguiente ventana, puede insertar y modificar los datos acorde a las necesidades de su organización. 
111.	Una vez finalizada la modificación de datos, pulse el botón "Guardar" para salvaguardar los datos modificados. 

2.4.6. ELIMINACIÓN DE DATOS

En este procedimiento se muestra a modo de ejemplo el método de eliminación de datos de una tabla.

Paso	Descripción
112.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
113.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**.

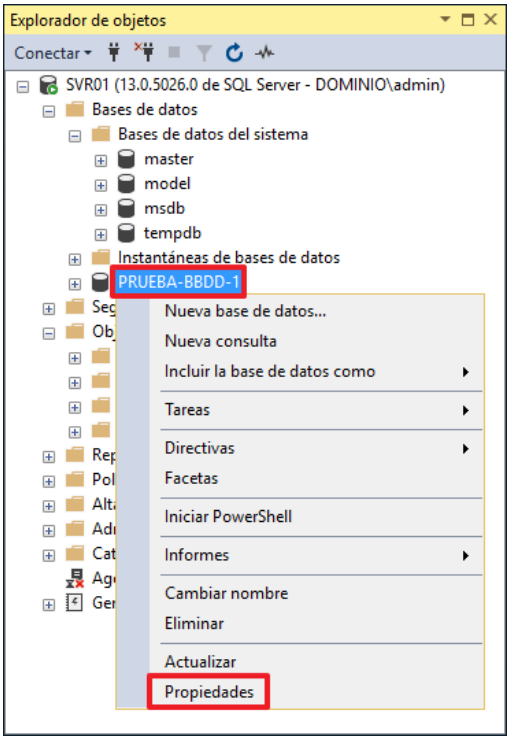
Paso	Descripción
114.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".
115.	Dentro del Explorador de objetos, expanda el árbol "Bases de datos" hasta llegar a la tabla que en la que desea eliminar un dato.  **Nota:** En este ejemplo, se utiliza la tabla "dbo.Clientes".
116.	Una vez seleccionada la tabla, haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Editar las 200 primeras filas" para insertar los datos en la tabla seleccionada. 
117.	Haga clic derecho sobre fila que desea eliminar y pinche sobre la opción del menú contextual "Eliminar" para borrar el registro seleccionado. 

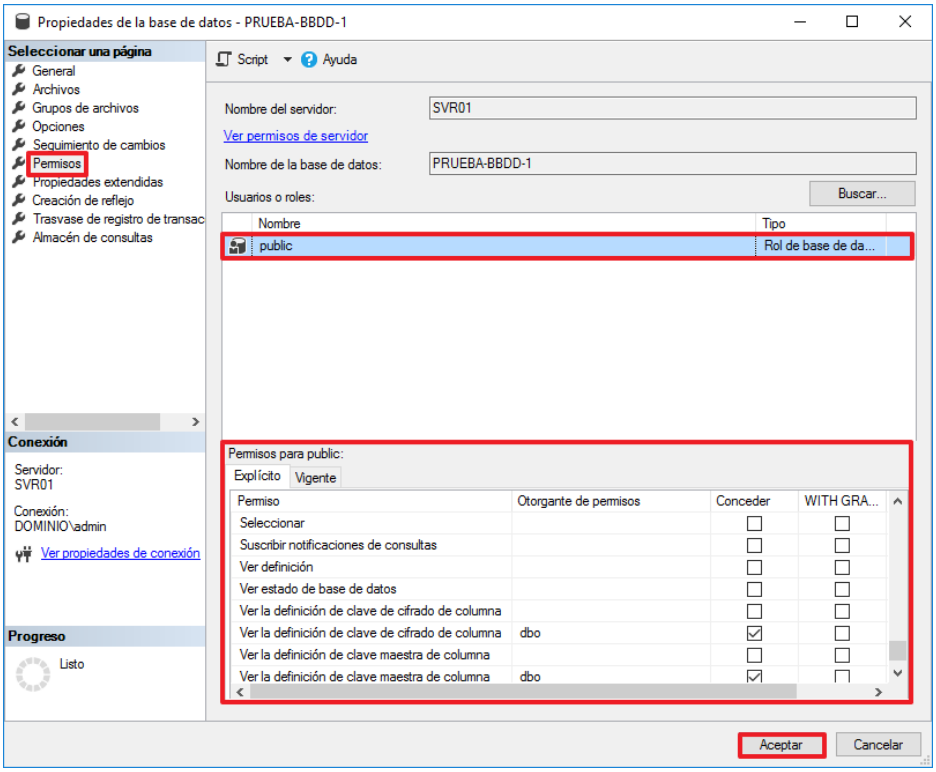
2.5. ASIGNACIÓN DE PERMISOS SOBRE SQL

Los permisos de acceso sobre los diferentes datos dentro de SQL Server 2016 deben quedar limitado a los usuarios legitimados para ello. Por lo tanto, será necesario establecer los permisos necesarios para limitar dicho acceso.

2.5.1. PERMISOS EN BASES DE DATOS

En este procedimiento se describen los procesos para alterar los permisos de diferentes objetos de la base de datos.

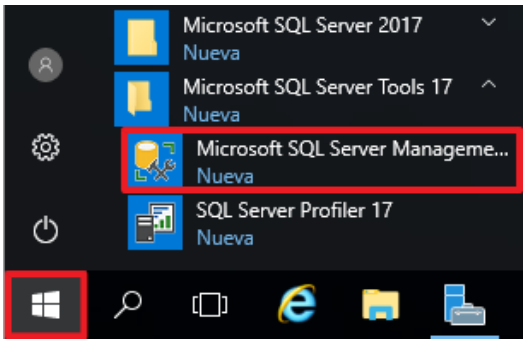
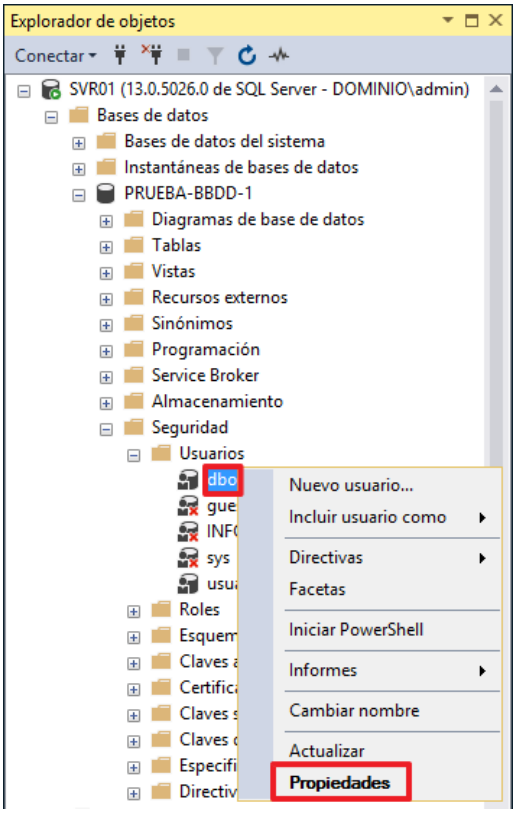
Paso	Descripción
118.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
119.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".**
120.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".
121.	Una vez seleccionada la tabla, haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Propiedades".  **Nota:** En este ejemplo, se utiliza la base de datos "PRUEBA-BBDD-1".

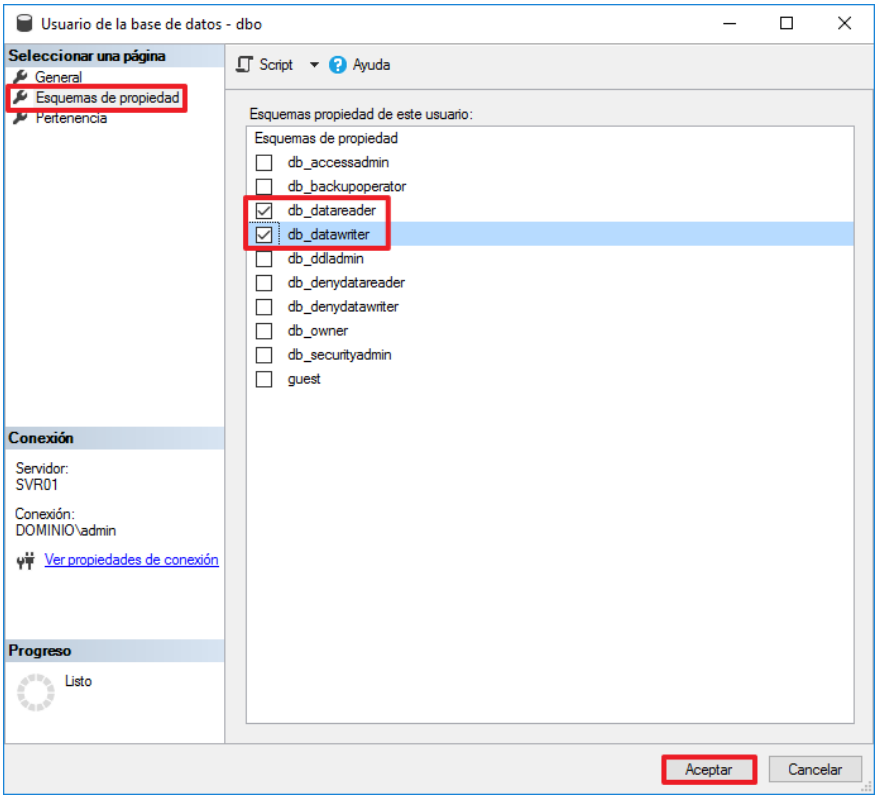
Paso	Descripción
122.	En la siguiente pantalla, seleccione en el menú de la izquierda la página "Permisos" y establezca los permisos necesarios a corde a su organización. Cuando haya finalizado pulse "Aceptar" para guardar los permisos configurados.  **Nota:** SQL Server posee una gestión de usuarios, roles, permisos y políticas sobre los objetos específicos contenidos en la base de datos dentro del servidor SQL. Dicha gestión se puede asignar mediante permisos de seguridad individuales para cada uno de estos objetos. Para más información sobre los permios en SQL Server 2016 consulte la siguiente página: https://docs.microsoft.com/es-es/sql/relational-databases/security/permissions-database-engine?view=sql-server-2016.

2.5.2. PERMISOS DE USUARIOS SOBRE BASES DE DATOS

En esta sección se definen los procesos para alterar los permisos de los diferentes usuarios sobre una base de datos.

Paso	Descripción
123.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.

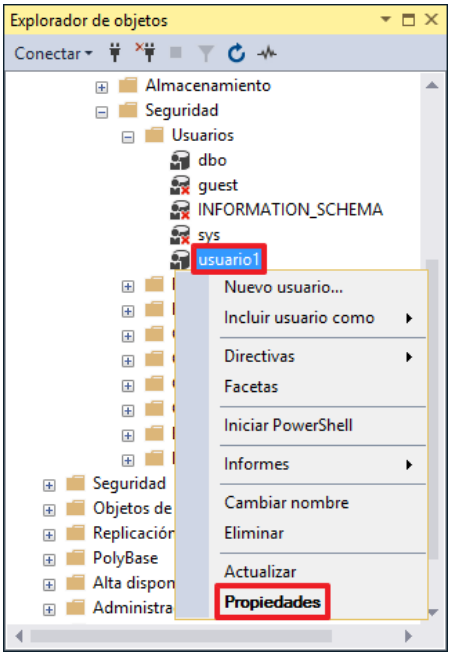
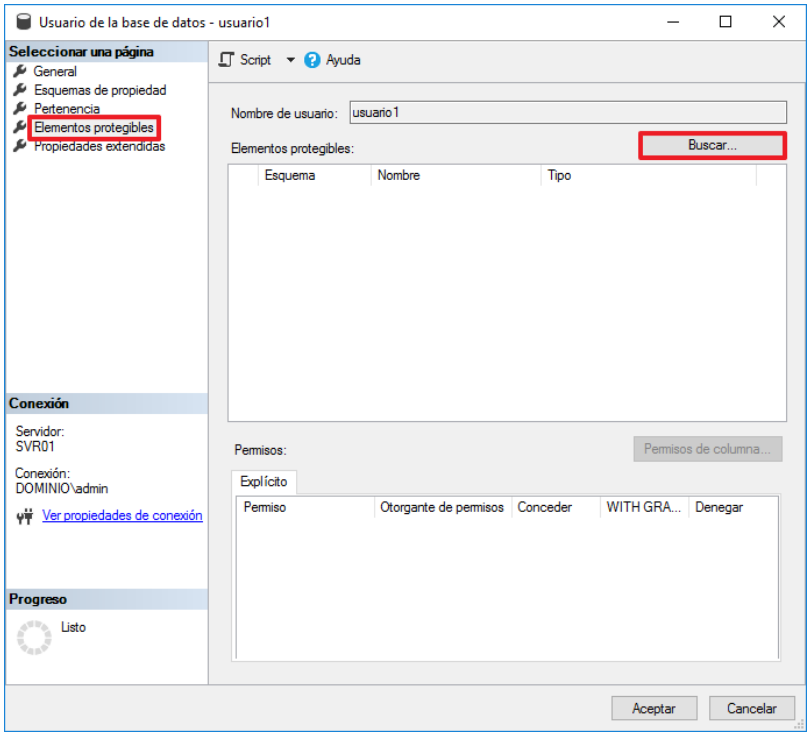
Paso	Descripción
124.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".** 
125.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".
126.	Una vez dentro de la consola de administración de SQL Server, expanda el árbol de su base de datos hasta llegar al siguiente nodo **"Bases de datos → <PRUEBA-BBDD-1> → Seguridad → Usuarios"** y desplegando el menú contextual con el botón derecho sobre el usuario que quiera administrar, seleccione la opción "Propiedades".  **Nota:** En este ejemplo, se utiliza el usuario "dbo" sobre la base de datos "PRUEBA-BBDD-1".

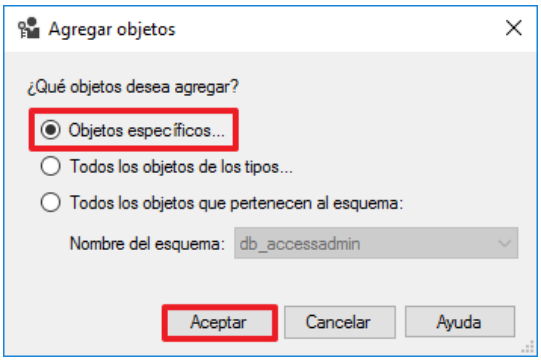
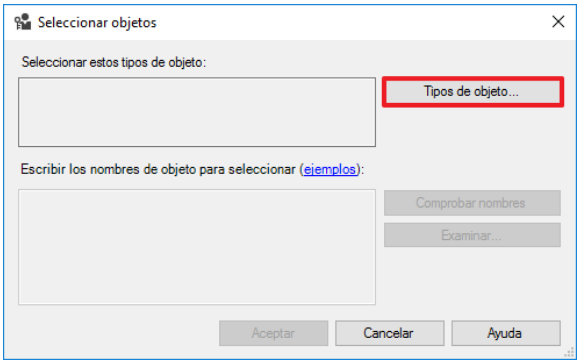
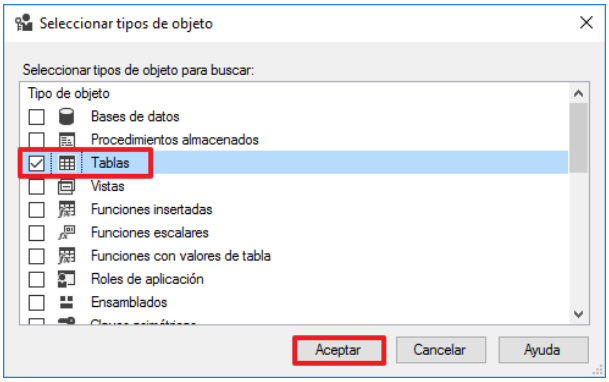
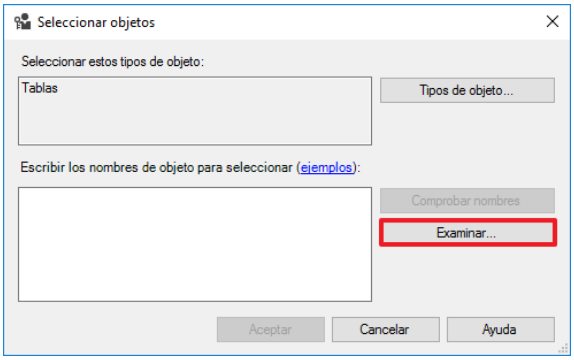
Paso	Descripción
127.	En la siguiente ventana, sitúese en el menú de la izquierda y pinche en la página "Esquemas de propiedad" y asigne los permisos de usuario sobre la base datos acorde a las necesidades de su organización y pulse "Aceptar".  **Nota:** En este ejemplo, se han asignado los permisos de lectura ("db_datareader") y modificación ("db_datawriter").

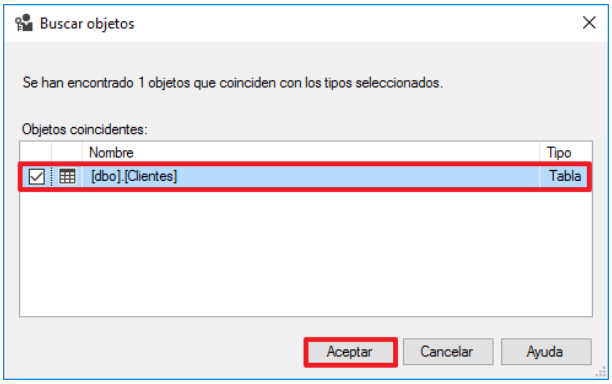
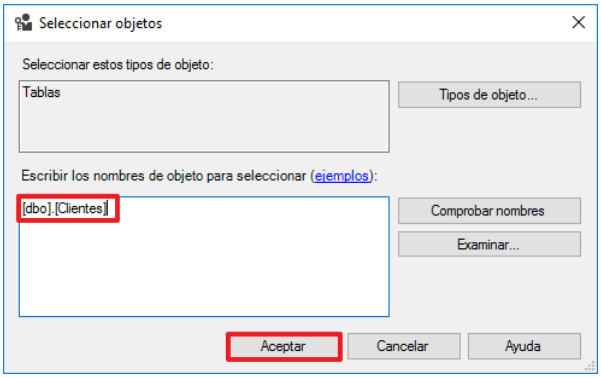
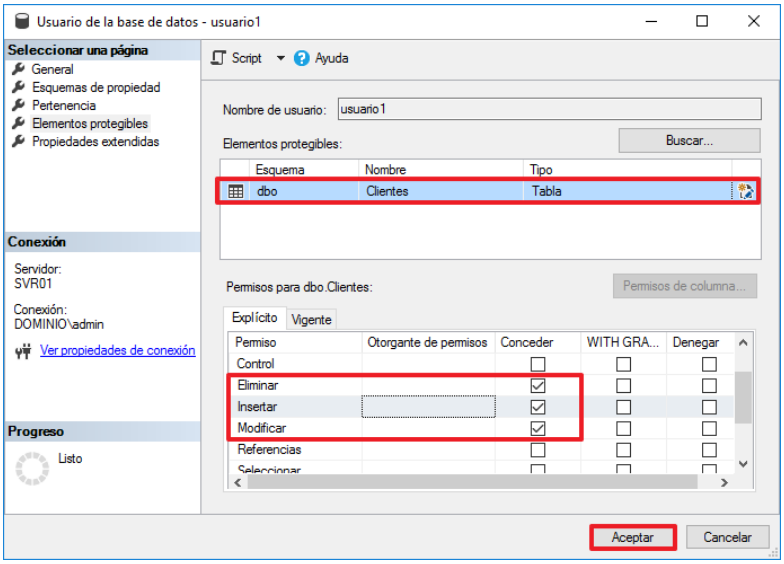
2.5.3. PERMISOS EN TABLAS

En este procedimiento se describen los procesos para cambiar permisos en las tablas.

Paso	Descripción
128.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
129.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".**
130.	En la ventana de "Conectar con el servidor", asegúrese de que el nombre del servidor es el correcto y pulse "Conectar".

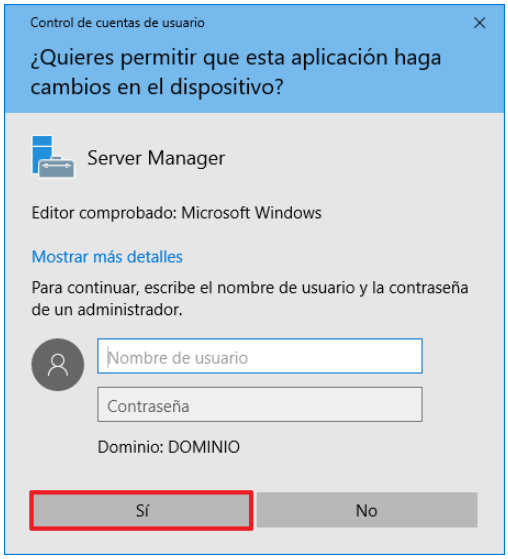
Paso	Descripción
131.	Una vez dentro de la consola de administración de SQL Server, expanda el árbol de su base de datos hasta llegar al siguiente nodo **"Bases de datos → <PRUEBA-BBDD-1> → Seguridad → Usuarios"** y desplegando el menú contextual con el botón derecho sobre el usuario que quiera administrar, seleccione la opción "Propiedades".  **Nota:** En este ejemplo, se utiliza el usuario "usuario1" sobre la base de datos "PRUEBA-BBDD-1".
132.	En la siguiente ventana, sitúese en el menú de la izquierda y pinche en la página "Elementos protegibles" y pulse sobre el botón "Buscar...". 

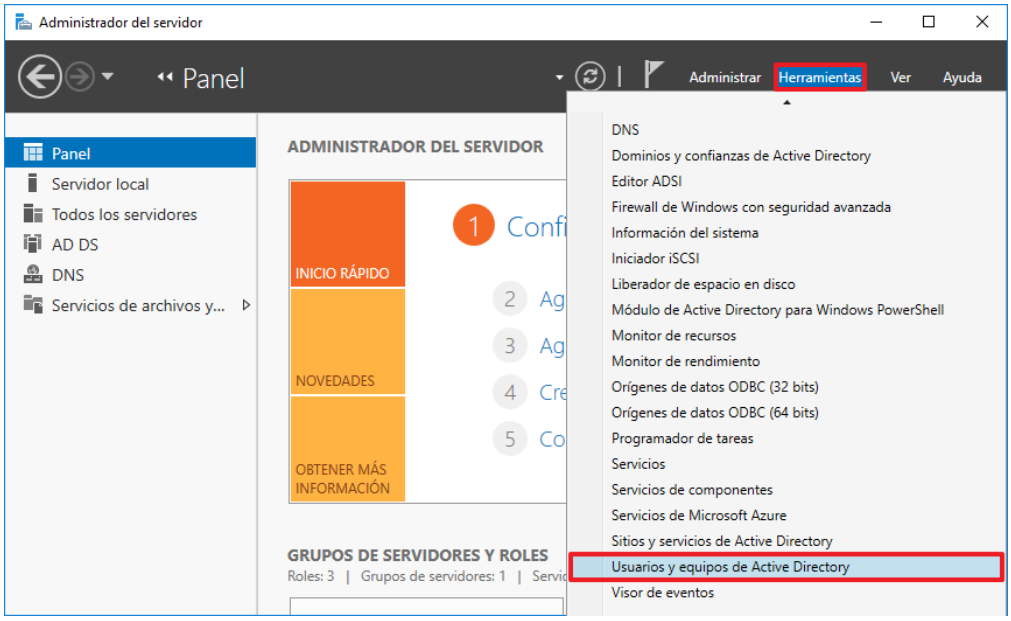
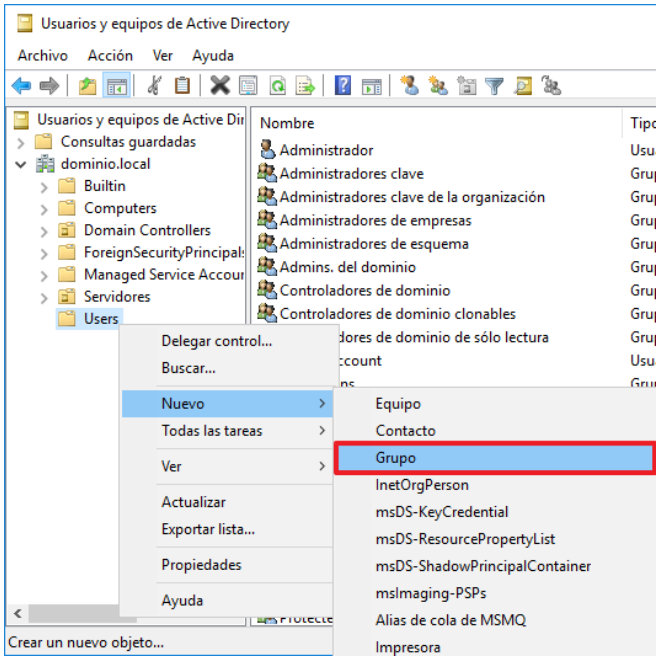
Paso	Descripción
133.	A continuación, seleccione "Objetos específicos…" y pulse "Aceptar". 
134.	En la siguiente ventana emergente, presione "Tipos de objeto…". 
135.	Seleccione el objeto "Tablas" y pulse "Aceptar". 
136.	A continuación, pulse el botón "Examinar…". 

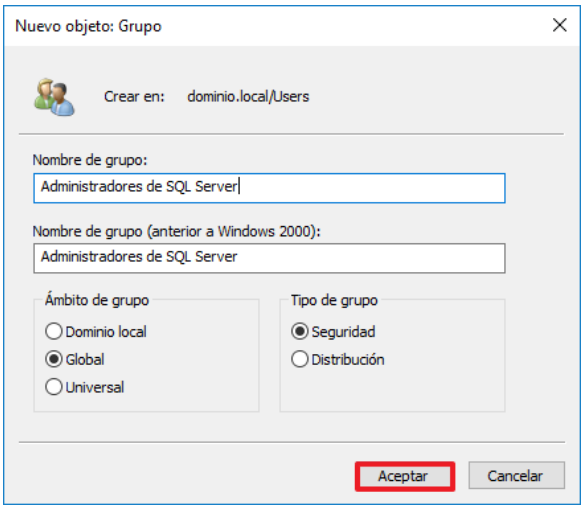
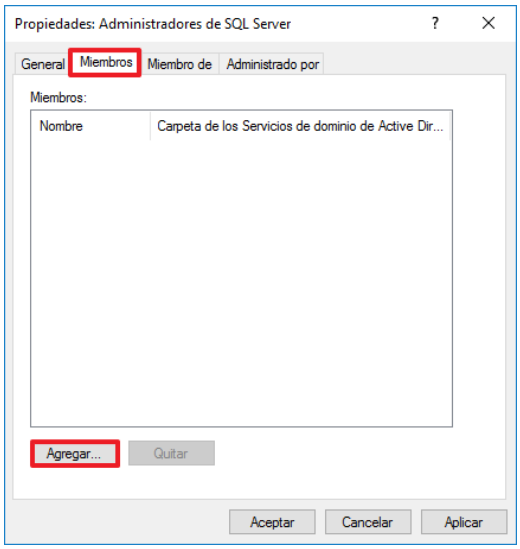
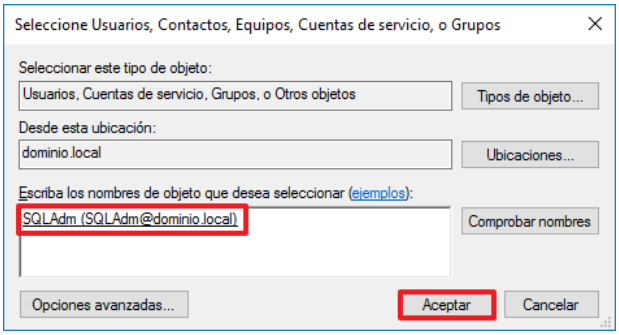
Paso	Descripción
137.	En la siguiente ventana emergente, seleccione la tabla que desea asignarle al usuario previamente establecido. 
138.	Para finalizar, compruebe que la tabla se ha asignado correctamente y vuelva a pulsar "Aceptar" para guardar los cambios. 
139.	En la parte inferior de la ventana, asigne los permisos al usuario sobre la tabla seleccionada acorde a las necesidades de su organización. Pulse "Aceptar" para guardar los cambios.  **Nota:** En este ejemplo, se han asignado los permisos de eliminar, insertar y modificar al usuario "usuario1" sobre la tabla "Clientes".

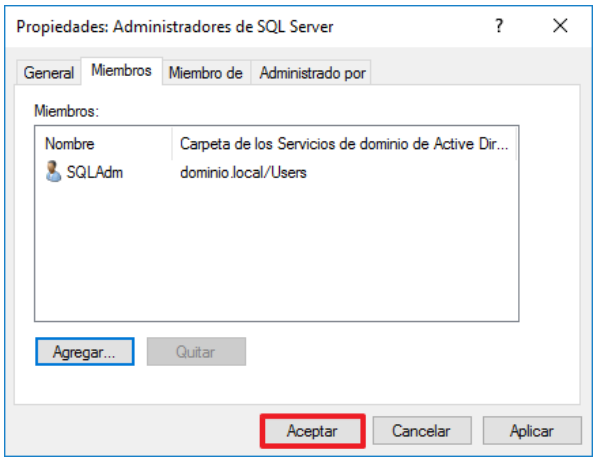
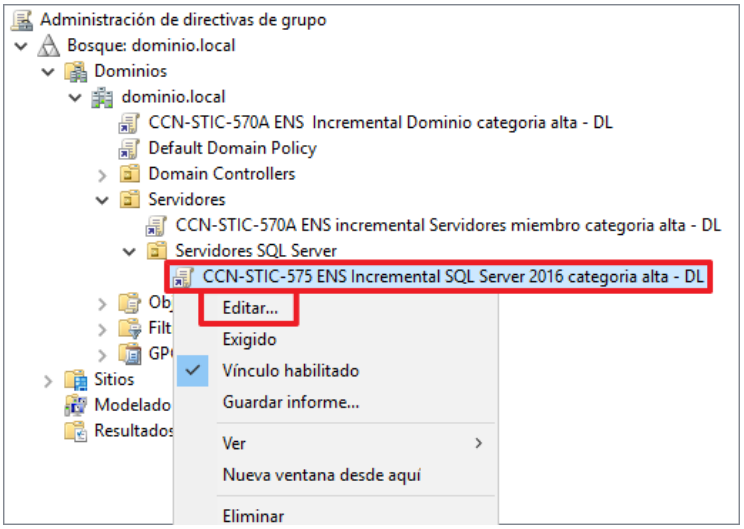
2.6. SEGREGACIÓN DE ROLES

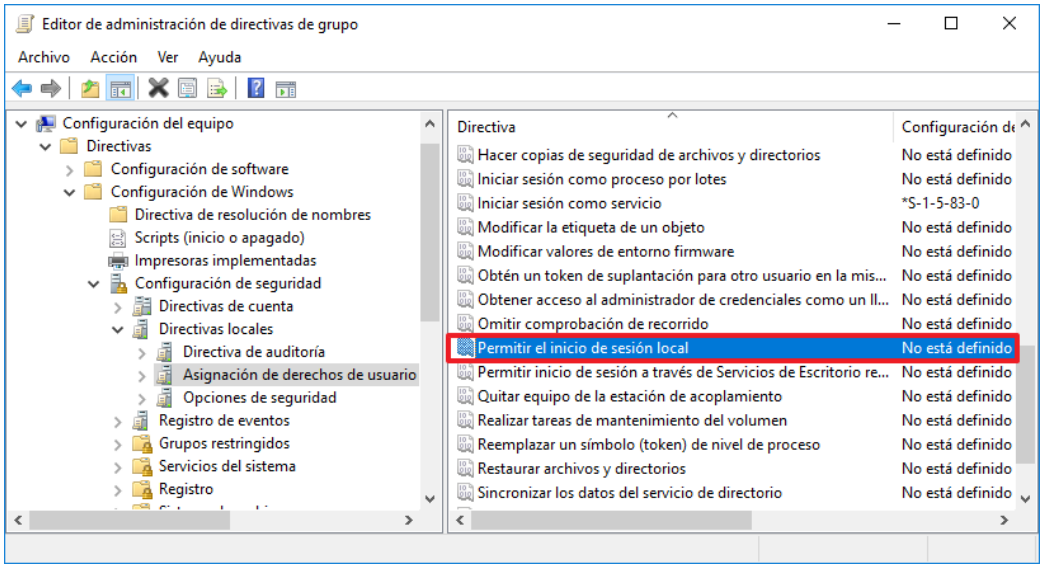
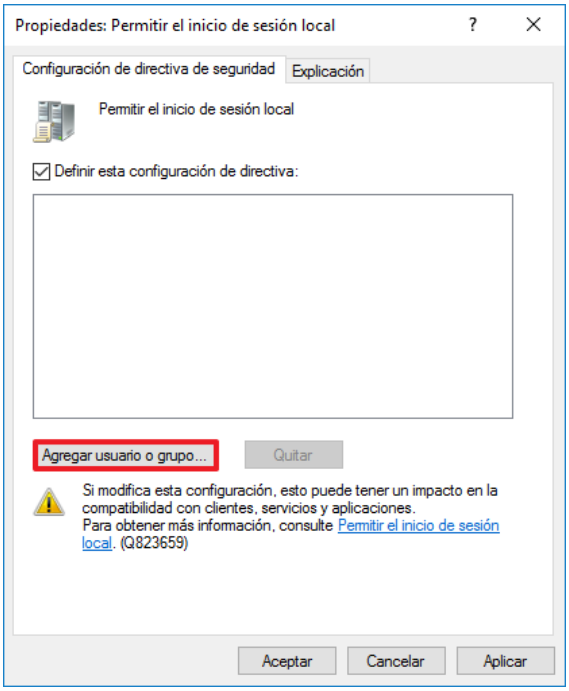
Con la aplicación del ENS para la categoría alta – DL sobre una un servidor SQL Server 2016 será necesario crear grupos de usuarios para conceder o denegar permisos sobre un recurso, así como administrar SQL Server 2016.

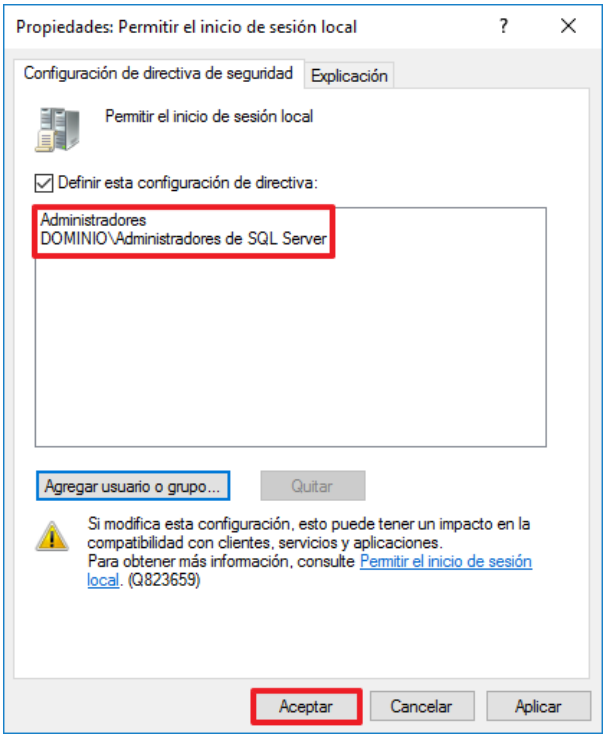
Paso	Descripción
140.	Inicie sesión en el servidor Controlador de Dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio.
141.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
142.	El "Control de cuentas de usuarios" le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador de dominio y pulse "Sí". 

Paso	Descripción
143.	Acceda al apartado "Herramientas" y seleccione "Usuarios y Equipos de Active Directory". 
144.	Despliegue el nodo **"<su dominio> → Users"**. Pulse con el botón derecho sobre "Users" y seleccione la opción del menú contextual **"Nuevo → Grupo"**. 

Paso	Descripción
145.	Establezca el nombre de grupo deseado para su organización y pulse "Aceptar".  **Nota:** En este ejemplo se utiliza el nombre "Administradores de SQL Server".
146.	Haga doble clic sobre el grupo recién creado y acceda a la pestaña "Miembros". Pulse sobre el botón "Agregar…" para añadir usuarios al grupo. 
147.	Añada los usuarios que desee al grupo y pulse "Aceptar".  **Nota:** En este ejemplo se añade el usuario "SQLAdm".

Paso	Descripción
148.	Pulse "Aceptar" cuando haya finalizado. 
149.	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".** 
150.	Acceda al nodo "Servidores de SQL Server", pulse con el botón derecho el objeto GPO denominado "CCN-STIC-575 ENS incremental SQL categoria alta - DL", creado en apartados anteriores y seleccione la opción del menú contextual "Editar…". 

Paso	Descripción
151.	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"**. 
152.	Marque la casilla "Definir esta configuración de directiva:" y pulse sobre "Agregar usuario o grupo…". 

Paso	Descripción
153.	Agregue el grupo "Administradores" y aquellos usuarios o grupos delegados para la administración del servidor SLQ Server 2016. Pulse "Aceptar" cuando haya finalizado.  **Nota:** En este ejemplo se hace uso del grupo denominado "Administración de SQL Server". Deberá adaptar esta configuración a las necesidades de su organización.
154.	Repita el proceso nuevamente a partir del paso "152 a 153" para las siguientes directivas: Depurar programas. Hacer copias de seguridad de archivos y directorios. Permitir el inicio de sesión local. La siguiente tabla muestra cómo deben quedar configuradas las directivas.

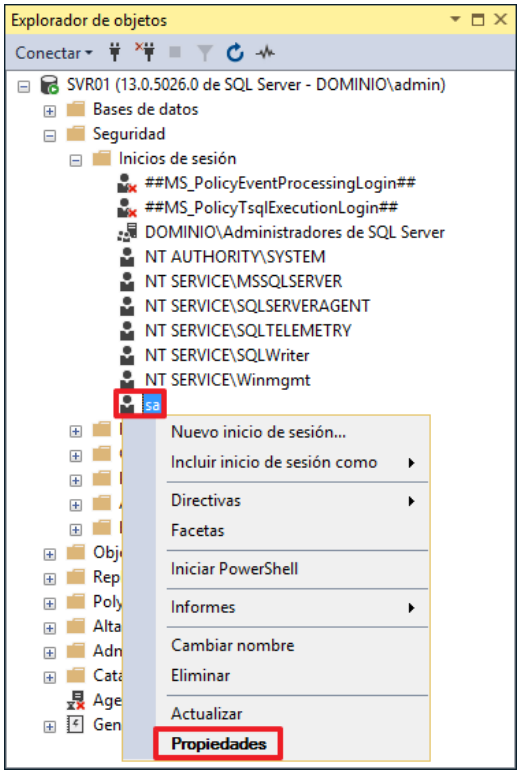
Directiva	Configuración de directiva
Administrar registro de seguridad y auditoría	Administradores DOMINIO\Administradores de SQL Server
Depurar programas	DOMINIO\Administradores de SQL Server
Hacer copia de seguridad de archivos y directorios	Administradores BUILTIN\Operadores de copia de seguridad DOMINIO\Administradores de SQL Server
Permitir el inicio de sesión local	Administradores DOMINIO\Administradores de SQL Server

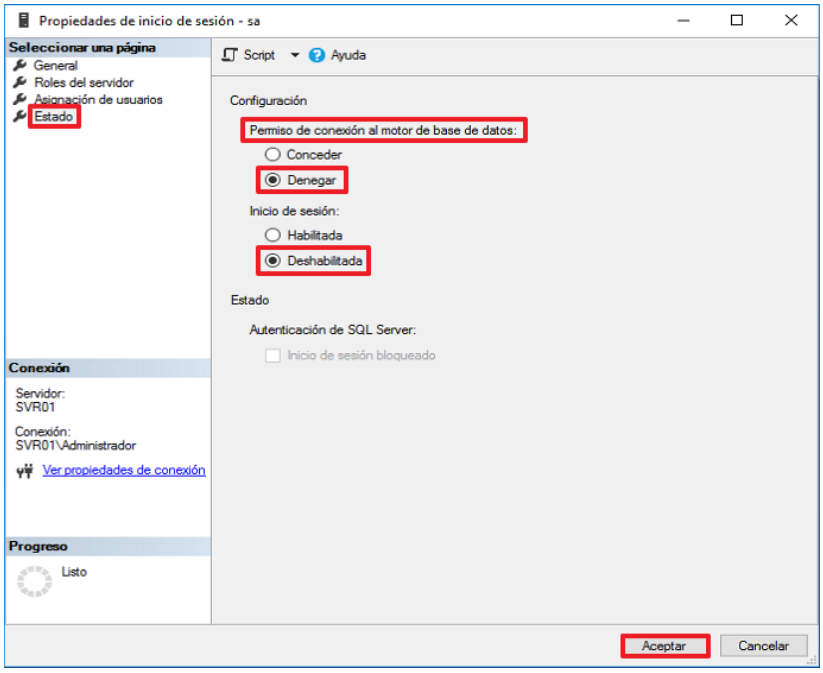
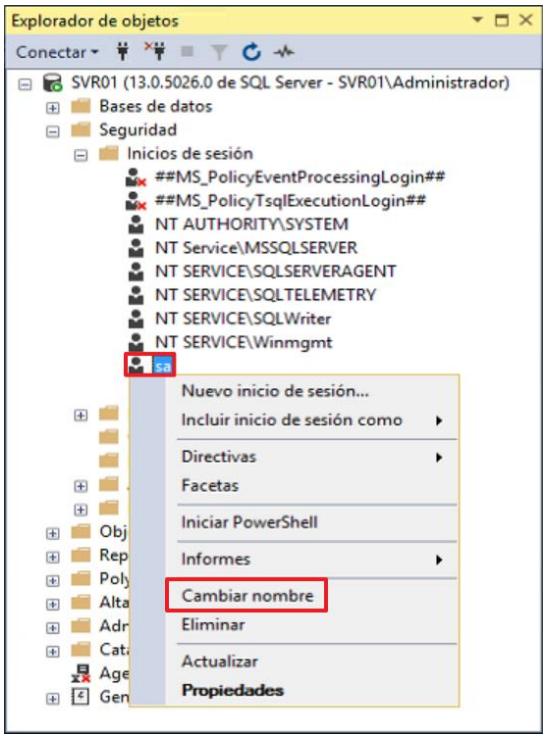
2.7. SEGURIDAD SOBRE EL USUARIO SA

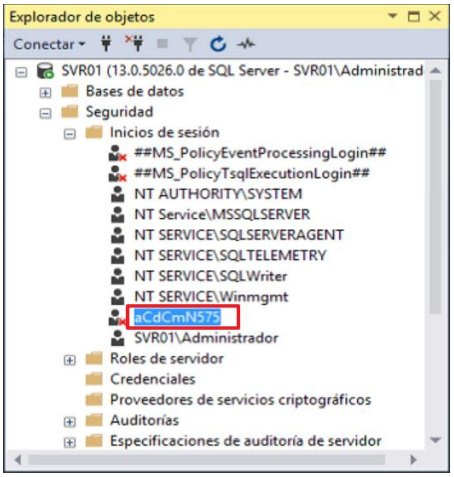
SQL Server 2016 instala de forma predeterminada un inicio de sesión denominado "sa" como abreviatura de "system administrator" ("administrador de sistema"). El inicio de sesión de "sa" se asigna al rol del servidor sysadmin, con lo que dispone de credenciales administrativas irrevocables en todo el servidor.

A continuación, en el siguiente punto se deshabilitará el inicio de sesión del usuario "sa" y se le asignará un nombre alternativo para impedir ataques de fuerza bruta sobre dicho usuario.

Nota: Antes de empezar, asegúrese de tener al menos una cuenta perteneciente al rol de servidor de "Sysadmin".

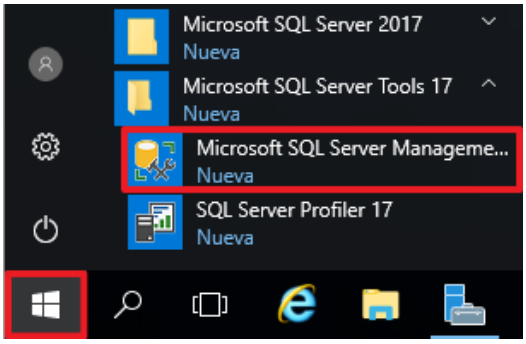
Paso	Descripción
155.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta que pertenezca al grupo "Administradores de SQL Server".
156.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".**
157.	En la ventana de "Conectar con el servidor", asegúrese de que el nombre del servidor es el correcto y pulse "Conectar".
158.	A continuación, despliegue el nodo **"Servidor: <<nombre del servidor>> → Seguridad → Inicios de sesión"** y desplegando el menú contextual con el botón derecho, seleccione la opción "Propiedades".  **Nota:** En este ejemplo, se utiliza el nombre del servidor "SVR01".

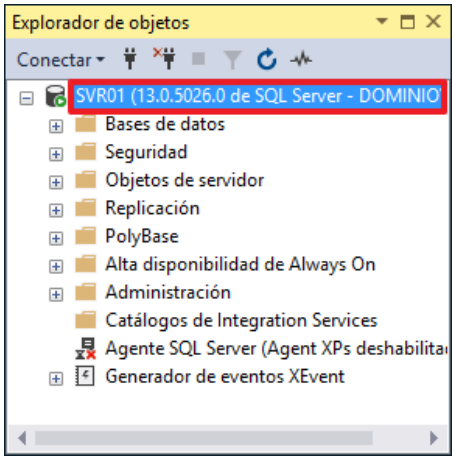
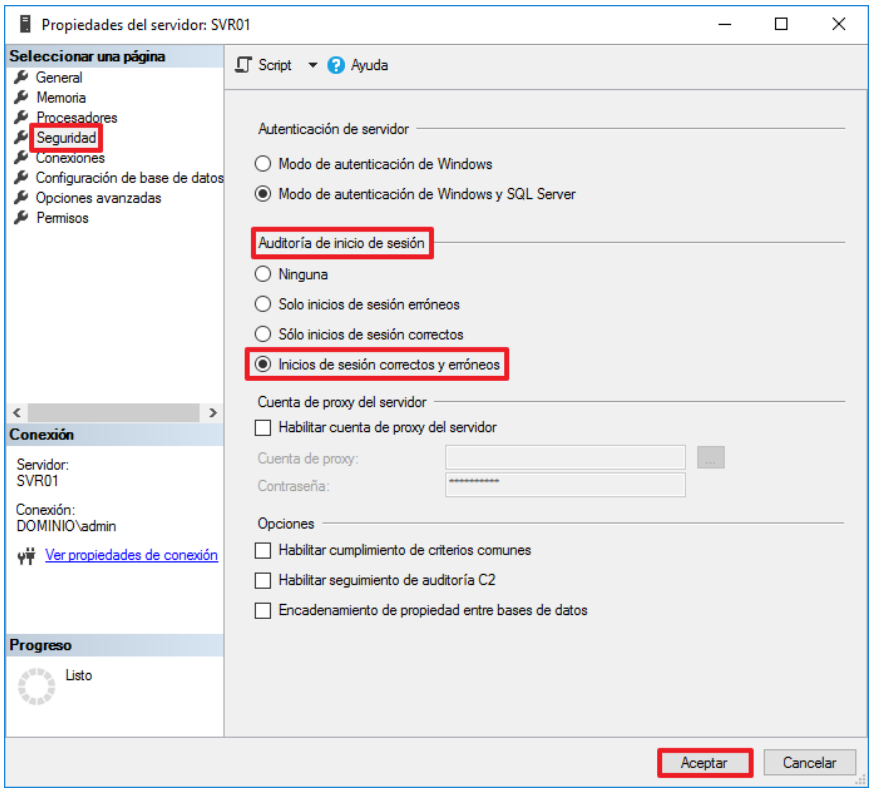
Paso	Descripción
159.	A continuación, sitúese en la página "Estado" dentro de la configuración "Permiso de conexión al motor de base de datos" y seleccione "Denegar". Repita el mismo proceso, pero en la configuración "Inicio de sesión" marcando la opción "Deshabilitada". Pulse "Aceptar" para guardar los cambios. 
160.	Una vez deshabilitado el usuario "sa", haga clic derecho sobre dicho usuario y desplegando el menú contextual, seleccione la opción "Cambiar nombre".  **Nota:** Verifique que el usuario "sa" aparece deshabilitado mediante una "X" de color rojo. Si no es así, pulse F5 para refrescar el explorador de objetos.

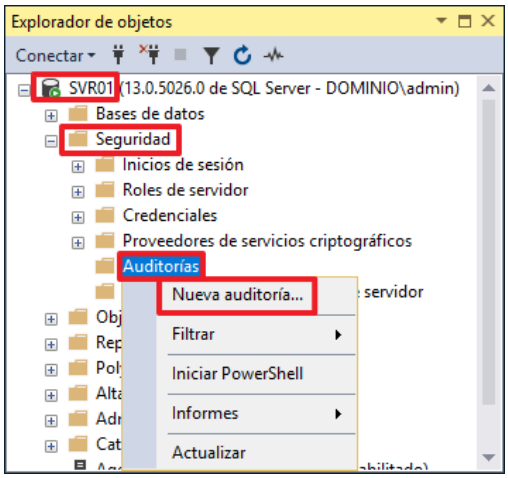
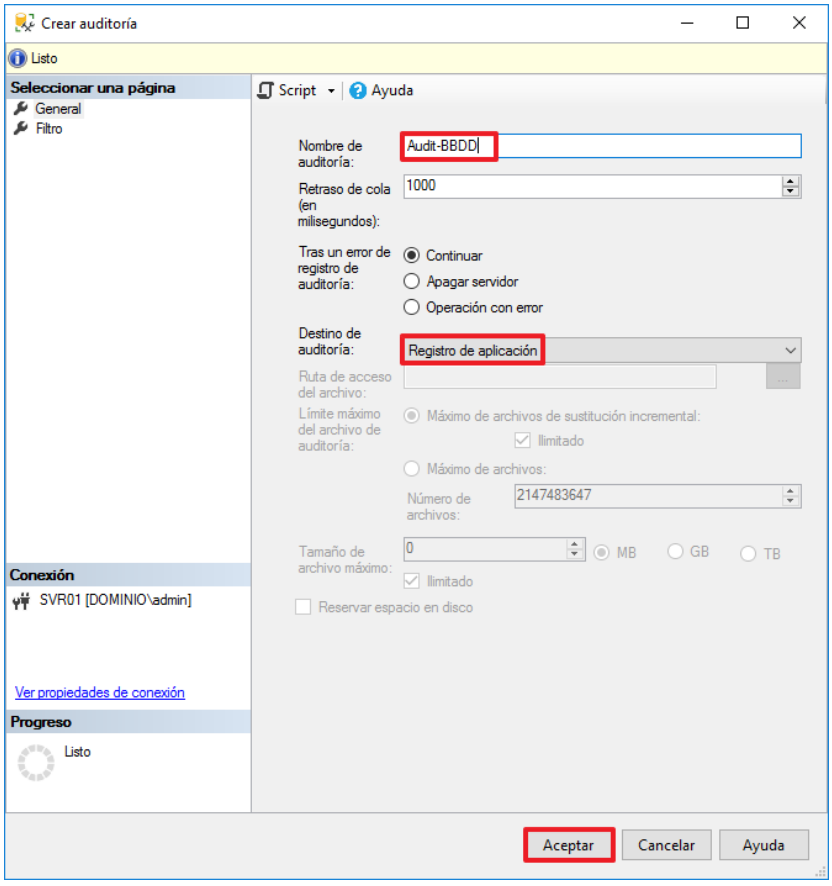
Paso	Descripción
161.	Establezca el nombre "aCdCmN575" para el usuario "sa". 

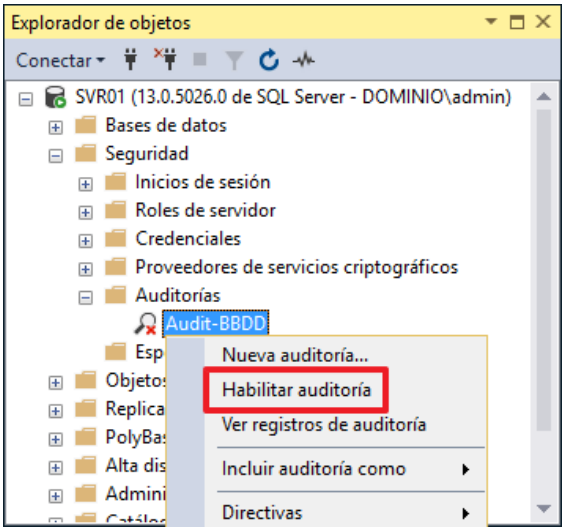
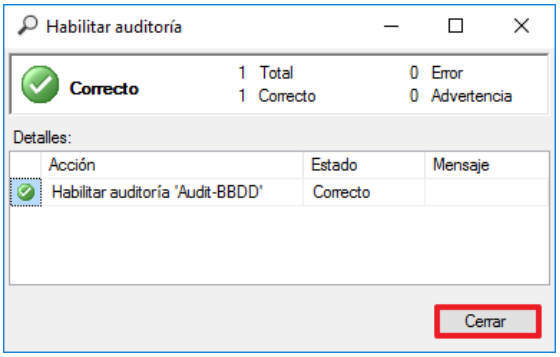
2.8. AUDITORÍA EN SQL SERVER 2016

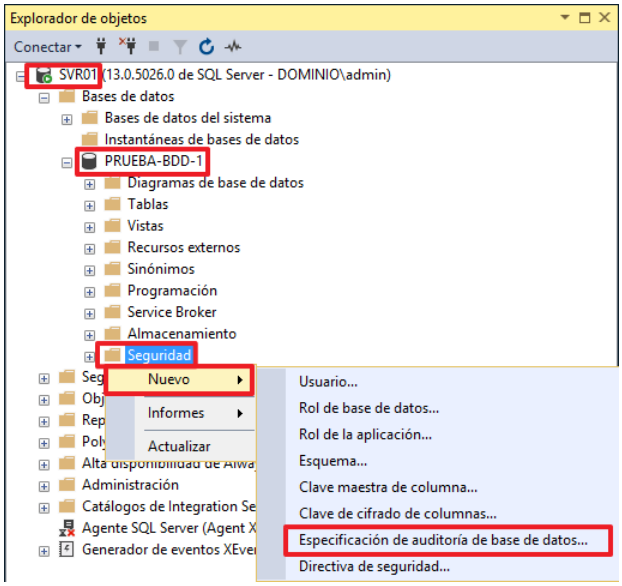
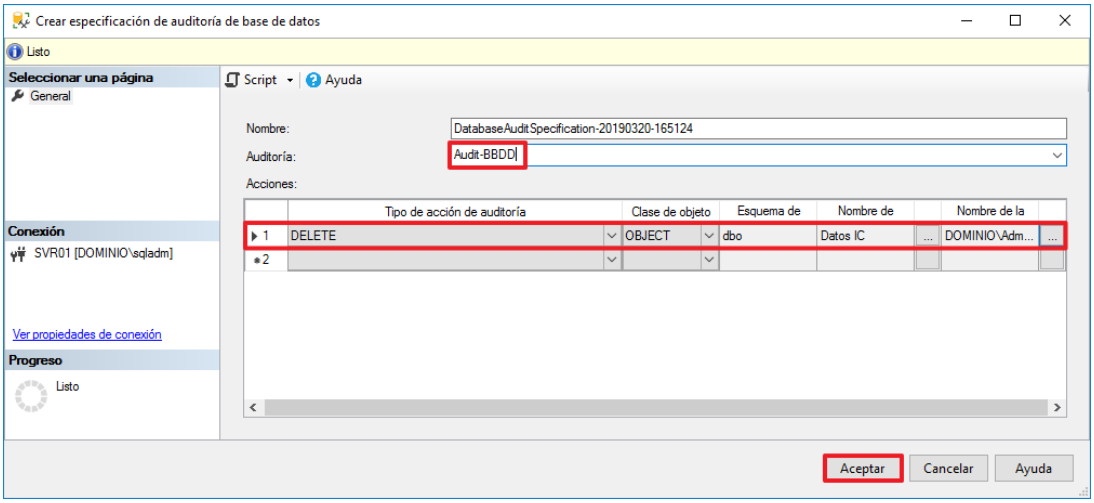
Existe la posibilidad que auditores lleven un control de las diferentes tareas que se realizan a través de SQL Server 2016. Esta sección recoge los pasos a seguir para realizar la configuración de una auditoria de eventos de un servidor de SQL Server 2016, así como de auditorías a nivel de bases de datos. Estos pasos se realizarán a través de un servidor SQL Server 2016.

Paso	Descripción
162.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
163.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
164.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".

Paso	Descripción
165.	Dentro del Explorador de objetos, seleccione su servidor de SQL Server y haga clic con el botón derecho sobre ella y seleccione la opción del menú contextual "Propiedades". 
166.	En la siguiente pantalla, seleccione en el menú de la izquierda la página "Seguridad" y en el apartado de "Auditoria de inicio de sesión" marque la opción "Inicios de sesión correctos y erróneos". Cuando haya finalizado pulse "Aceptar" para guardar los permisos configurados. 

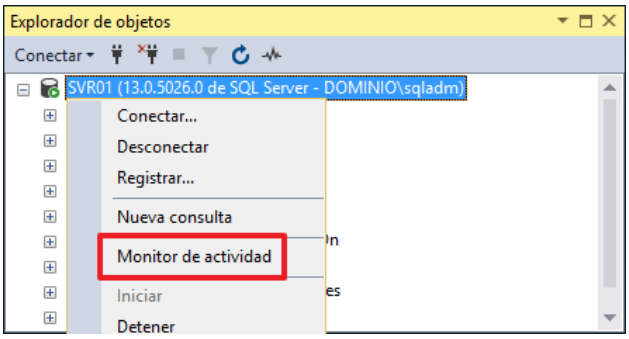
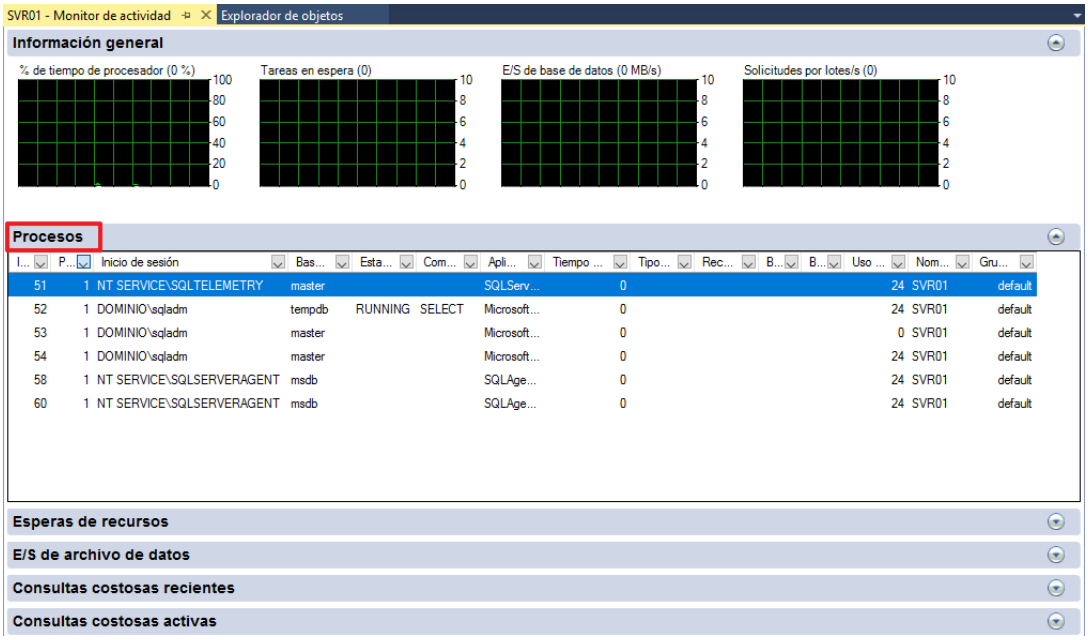
Paso	Descripción
167.	A continuación, despliegue el nodo **"Servidor: <<nombre del servidor>> →Seguridad →Auditorías"** y desplegando el menú contextual con el botón derecho, seleccione la opción **"Nueva auditoria".**  **Nota:** En este ejemplo se utiliza el servidor con el nombre "SVR01".
168.	En la siguiente ventana de auditoria, establezca un nombre para el registro de auditoria y defina el parametro "Registro de aplicación" como destino de auditoria. Pulse "Aceptar" para guardar los cambios.  **Nota:** En este ejemplo se utiliza el nombre de auditoria "Audit-BBDD".

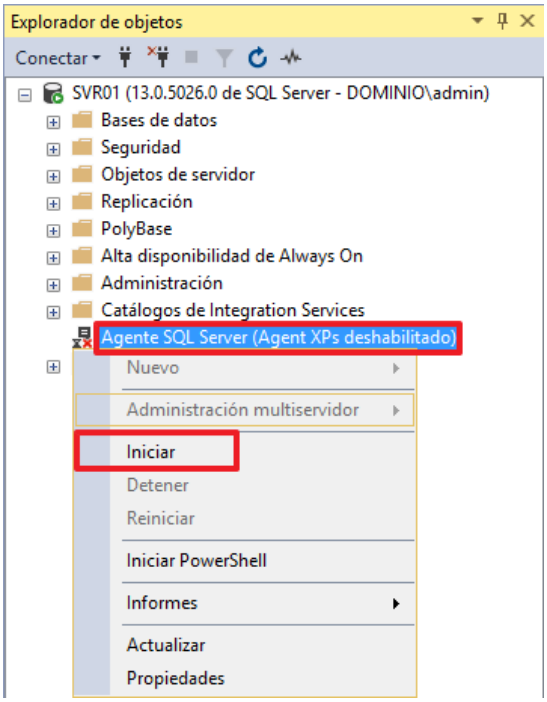
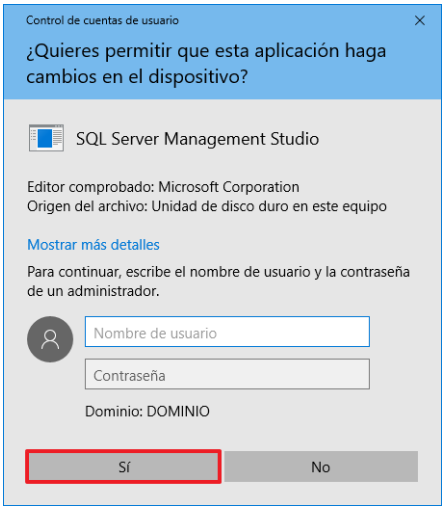
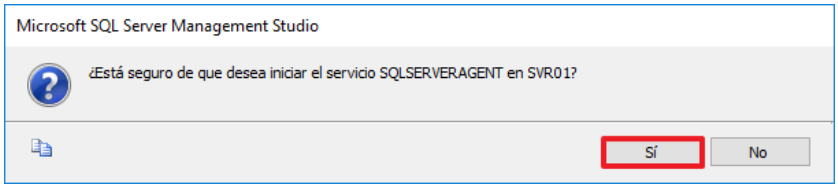
Paso	Descripción
169.	Ahora, seleccione la auditoria recien creda y desplegando el menú contextual con el botón derecho, seleccione la opción "Habilitar auditoria". 
170.	Una vez finalizado el proceso, verifique que el estado de la acción sea correcto y pulse "Cerrar". 
171.	Las auditorías pueden generarse a nivel de servidor o de base de datos. En estas ultimas, se puede establecer una auditoria a nivel de objetos de la base datos, como por ejemplo, auditar el evento "DELETE" en una base de datos especifica contra un inicio de sesión concreto. Para ello, se utilizara la auditoria creda anteriormente para trazar una auditoria de objetos.

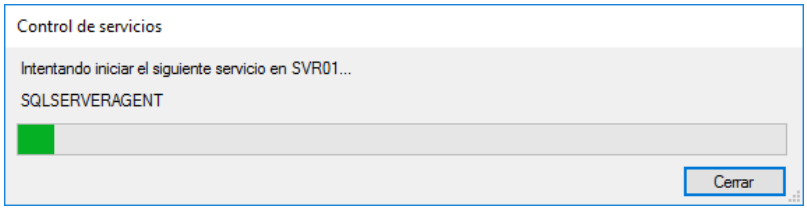
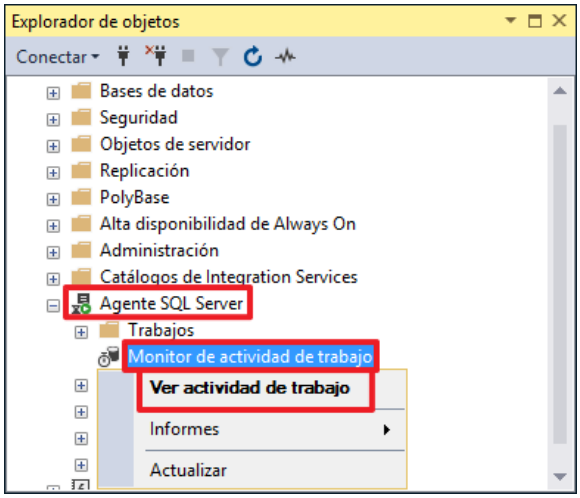
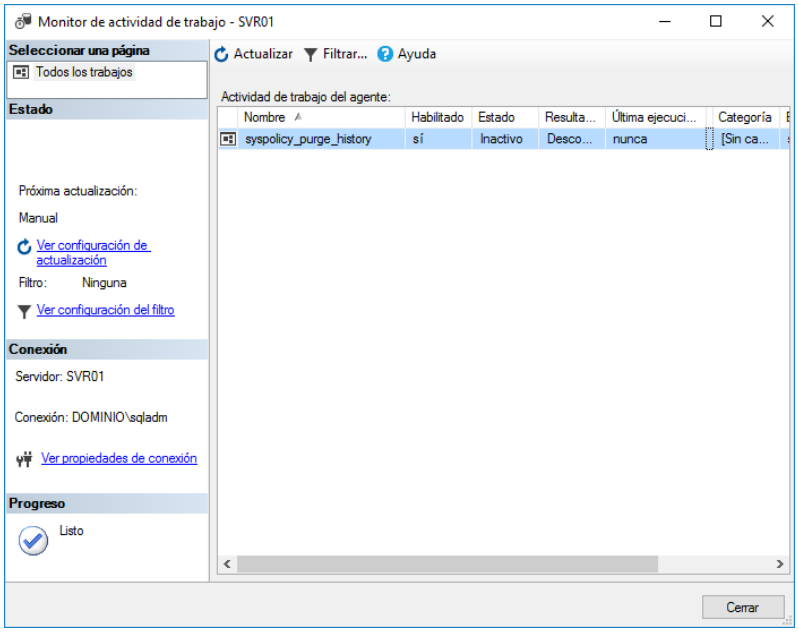
Paso	Descripción
172.	A continuación, despliegue el nodo **"Servidor: <<nombre del servidor>> → Bases de datos → Base de datos: <<nombre de la base de datos>> → Seguridad"** y desplegando el menú contextual con el botón derecho, seleccione la opción **"Nuevo → Especificación de auditoria de la base de datos…"**. 
173.	En la siguiente pantalla, establezca un tipo de auditoria, clase de objeto, nombre de la tabla de la base de datos y el nombre de la auditoria creada en pasos anteriores. Pulse "Aceptar" para guardar los cambios.  **Nota:** En este ejemplo, se establece una tipo de auditoria de objeto "DELETE" sobre la tabla "Datos IC" para el grupo de inicio de sesión "Administradores de SQL". Recuerde que solo los usuarios con el permiso "ALTER ANY DATABASE AUDIT" pueden crear especificaciones de auditoria de base de datos y enlazarlas a cualquier auditoria.

2.9. MONITORIZACIÓN DE LA ACTIVIDAD DE SQL

En SQL Server 2016 se puede monitorizar las acciones en las bases de datos en tiempo real, así como las actividades de trabajo por parte de cualquier usuario.

Paso	Descripción
174.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
175.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17".**
176.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".
177.	Dentro del Explorador de objetos, haga clic derecho sobre **"Servidor: <<nombre del servidor>>"** y desplegando el menú contextual seleccione la opción "Monitor de actividad". 
178.	En la siguiente ventana, dentro de la pestaña de "Procesos", podrá observar cada inicio de sesión activo en tiempo real. 

Paso	Descripción
179.	Para poder visualizar la actividad de los Jobs deberá iniciar el servicio SQLSERVERAGENT. Para ello, despliegue el nodo **"Servidor: <<nombre del servidor>> → Agente SQL Server (Agent XPs deshabilitado)"** y abriendo el menú contextual con el botón derecho, seleccione la opción "Iniciar". 
180.	El "Control de cuentas de usuarios" le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse "Sí". 
181.	Pulse "Sí" para iniciar el servicio de SQLSERVERAGENT. 

Paso	Descripción
182.	Tras unos segundos, se iniciará dicho servicio. 
183.	A continuación, navegue hasta el nodo **"Agente SQL Server → Trabajos → Monitor de actividad de trabajo"** y desplegando el menú contextual con el botón derecho, seleccione la opción "Ver actividad de trabajo". 
184.	En la pantalla monitor de actividad podrá observar el histórico y estado actual de los Jobs del servidor. 

2.10. CIFRADO DE CONEXIONES

Microsoft SQL Server 2016 siempre cifra los paquetes de red asociados al inicio de sesión. Si no se ha proporcionado ningún certificado en el servidor cuando éste se inicia, SQL Server genera un certificado autofirmado que utiliza para cifrar dichos paquetes.

Una vez establecida la conexión, las aplicaciones pueden solicitar el cifrado de todo el tráfico a través de palabras claves en las cadenas de conexión. Es necesario tener en cuenta que la configuración de estas cadenas de conexión nunca reduce el nivel de seguridad establecido por el administrador de configuración cliente de SQL Server.

Si se activa el cifrado, SQL Server cifra las comunicaciones realizando el cifrado SSL (40 bits o 128 bits dependiendo del sistema operativo) del payload del protocolo TDS (Tabular Data Stream). Es posible activar el cifrado del protocolo incluso cuando no se ha instalado un certificado en el servidor, utilizando en este caso el certificado autofirmado generado automáticamente por el servidor, lógicamente en este caso el cliente no puede validar el mismo.

Para aquellas organizaciones donde no se disponga de una entidad de certificación interna o infraestructura de clave pública (PKI), el certificado autofirmado generado por SQL Server puede ser suficiente para garantizar unos niveles mínimos de seguridad y la única acción a realizar sería la de forzar el cifrado en la instancia SQL Server.

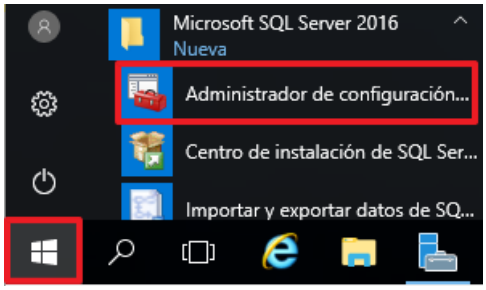
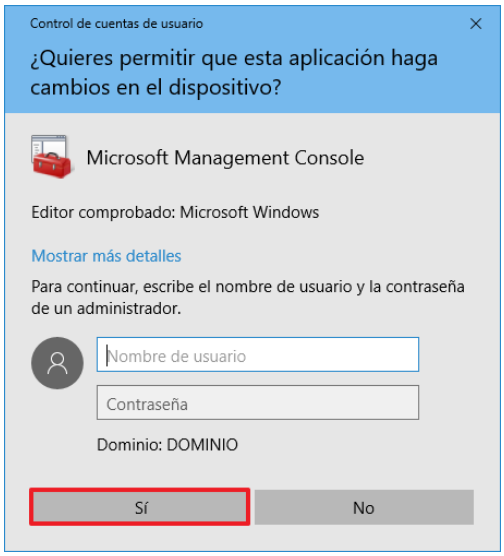
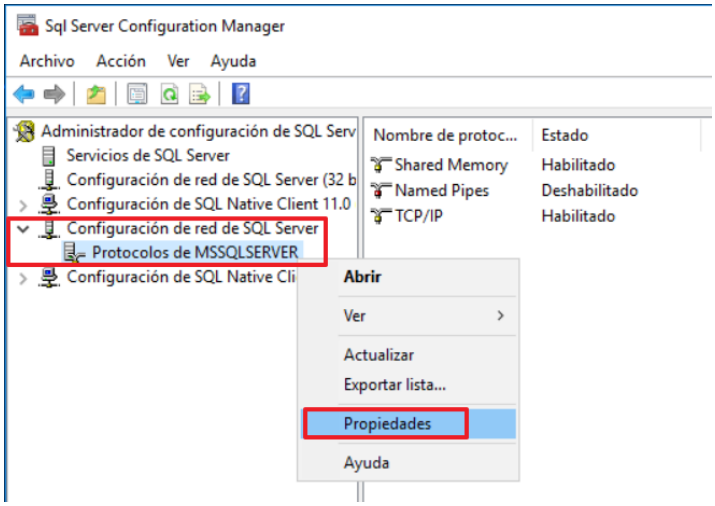
Sin embargo, el certificado autofirmado no es el más recomendable a la hora de implementar mecanismos de seguridad que requieran la confianza de los equipos clientes desde los que se va a acceder a SQL Server, ya que es relativamente sencillo suplantar la identidad de un certificado de estas características. Para evitar esto, se requiere la emisión e instalación de un certificado de seguridad que este firmado por una Entidad de Certificación autorizada y de confianza, ya sea interna o externa a la organización.

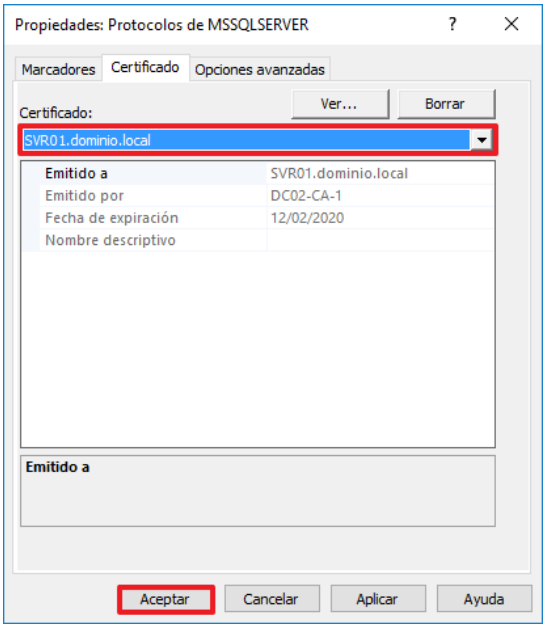
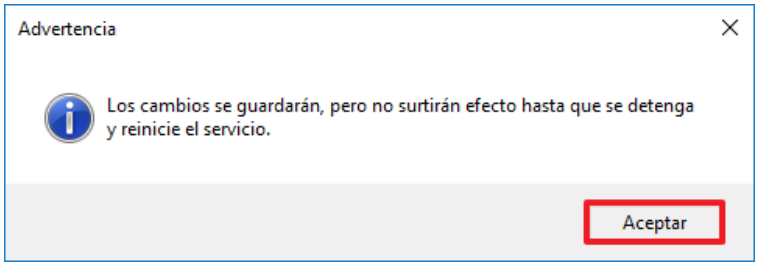
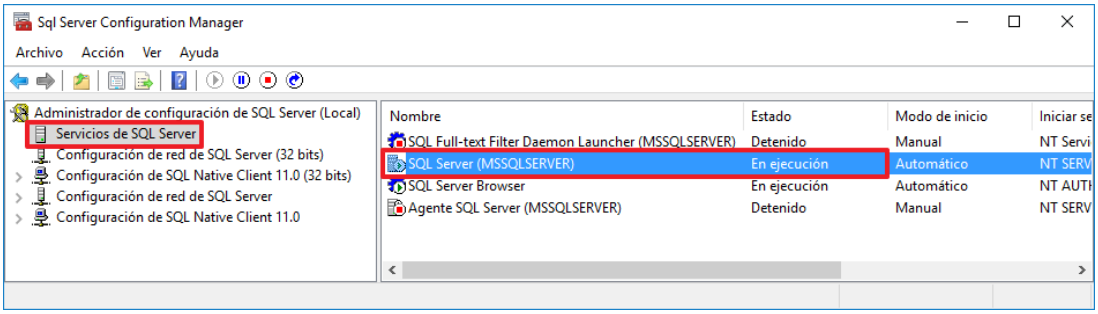
La implementación de certificados puede realizarse bien empleando certificados emitidos por una entidad certificadora que la organización haya implementado o bien por un certificado adquirido a través de una entidad certificadora de terceros como la FMNT (Fábrica Nacional de Moneda y Timbre).

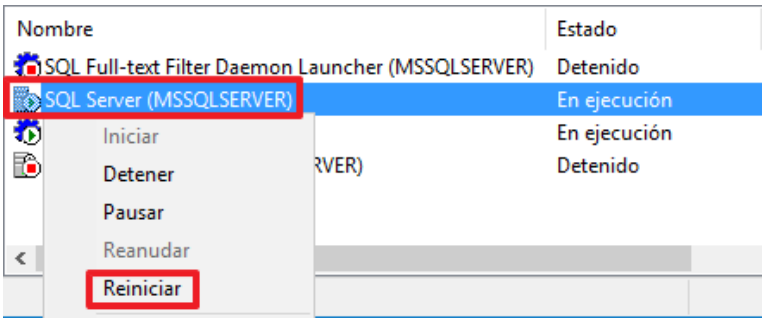
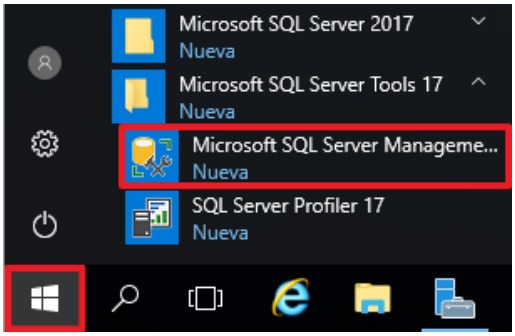
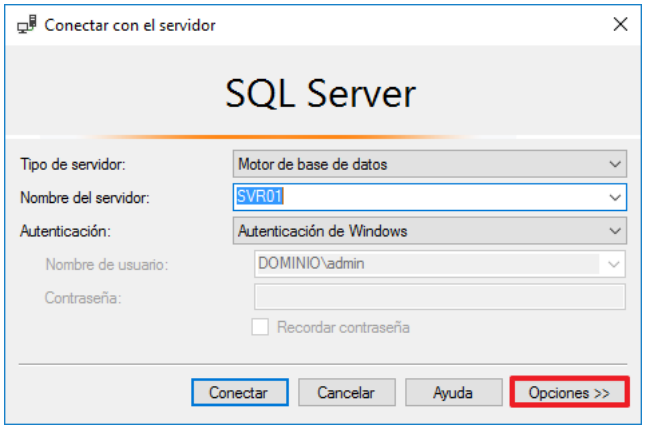
2.10.1. CONFIGURACIÓN DEL CIFRADO SSL EN EL SERVIDOR DE SQL SERVER

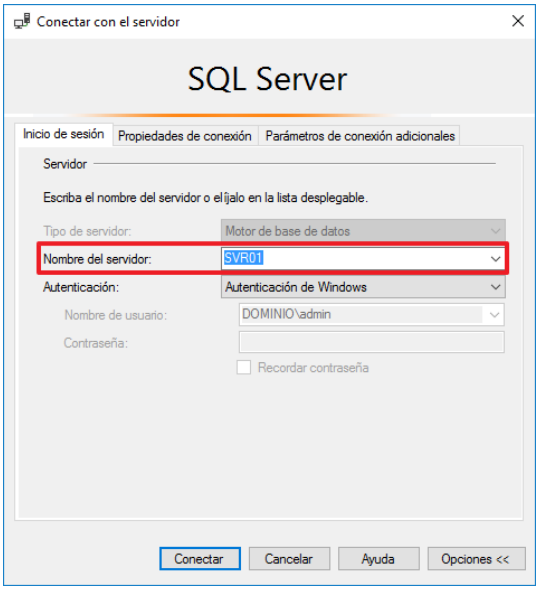
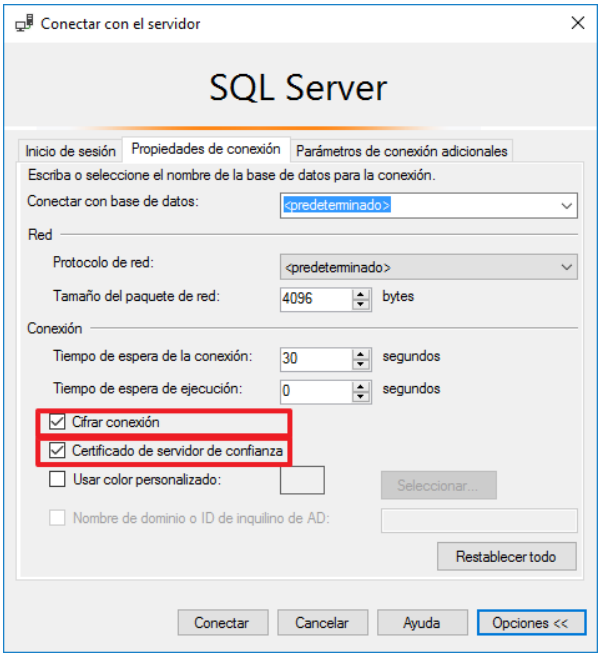
Una vez instalado correctamente el certificado en el servidor, con el objetivo de mejorar la seguridad de las comunicaciones de clientes y servidor, es necesario configurar la instancia de SQL Server 2016 para que haga uso del mismo.

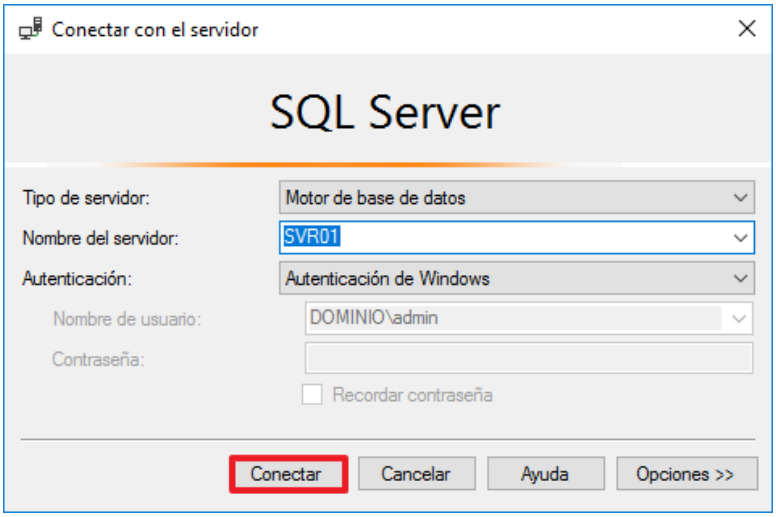
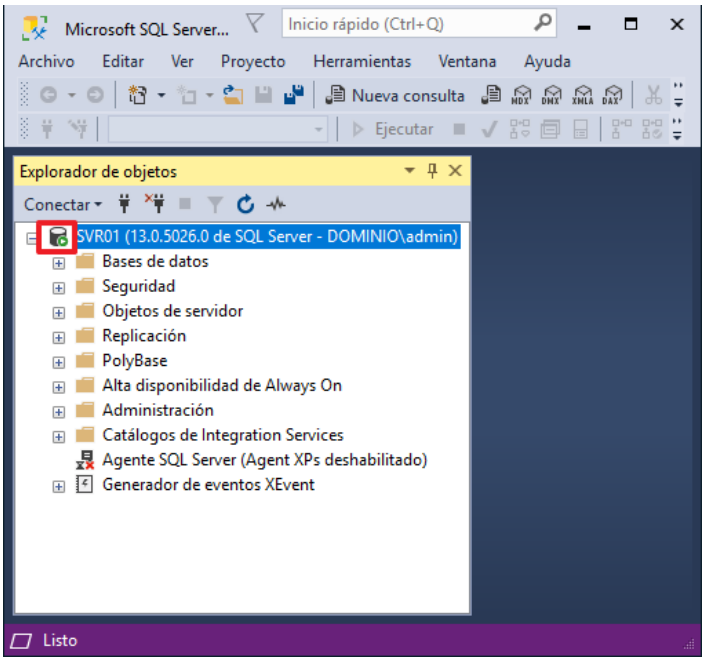
Paso	Descripción
185.	Inicie sesión en el servidor SQL Server 2016 servidor del dominio. **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

Paso	Descripción
186.	Inicie el administrador de Administrador de configuración de SQL Server 2016 desde **"Inicio → Herramientas administrativas → Microsoft SQL Server 2016 → Administración de configuración".** 
187.	El "Control de cuentas de usuarios" le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador de dominio y pulse "Sí". 
188.	En la consola de administración sitúese sobre el nodo **"Configuración de red de SQL Server → Protocolos de red de SQL Server"** haga clic con el botón derecho y seleccione la opción "Propiedades". 

Paso	Descripción
189.	En la ventana de propiedades de los protocolos de MSSQLSERVER, sitúese en la pestaña "Certificado" y seleccione del desplegable el certificado instalado anteriormente, pulse sobre el botón "Aceptar".  **Nota:** En la pestaña "Marcadores" es posible forzar el cifrado del protocolo desde el servidor, sin embargo, si se utiliza esta característica el servidor SQL Server pasará a utilizar el certificado autofirmado, por ello, se mantiene su valor en no, siendo las aplicaciones clientes las que fuerzan la conexión cifrada con validación de certificado.
190.	El sistema alerta de que los cambios se guardaran, pero que no sufrirán efecto hasta que se detenta y reinicie el servicio. Pulse sobre el botón "Aceptar". 
191.	Sitúese en el nodo "Servicios de SQL Server" en la consola del Administrador de configuración de SQL Server y localice el servicio SQL Server (MSSQLSERVER). 

Paso	Descripción
192.	Haga clic con el botón derecho sobre él y seleccione la opción "reiniciar" para detener e iniciar el servicio con la nueva configuración.  **Nota:** Para que el servicio inicie sin problemas es necesario que el certificado utilizado este emitido por una entidad de certificados de confianza en el servidor SQL Server.
193.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**. 
194.	Cuando se inicie SQL Server Management Studio, se mostrará una ventana de conexión hacia el SQL Server, pulse sobre la pestaña "Opciones >>" para establecer una configuración adecuada. 

Paso	Descripción
195.	Sobre la pestaña "Inicio de sesión", establezca el nombre del servidor SQL Server. 
196.	Dentro de la pestaña "Propiedades de Conexión", marque la opción "Cifrar conexión" y "Certificado de servidor de confianza".  **Nota:** Las máquinas clientes desde donde se establece la conexión cifrada al servidor SQL Server deben confiar en la entidad emisora del certificado. En caso contrario se producirá un error con el siguiente mensaje: "Se ha establecido la conexión con el servidor correctamente. Pero se ha producido un error durante el inicio de sesión previo del protocolo de enlace (provider: Proveedor de SSL, error: 0 – La cadena de certificación fue emitida por una entidad en la que no se confía).

Paso	Descripción
197.	Pulse sobre "Conectar" para establecer una conexión con el SQL Server. 
198.	Como puede observar en la siguiente imagen, el servidor SQL está funcionando correctamente. Verifique que aparece en su servidor SQL el icono verde de ejecución. 

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

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad para SQL Server 2016 sobre Microsoft Windows Server 2016 con implementación de seguridad de categoría básica 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 la sección de la guía "ANEXO A.4.1 PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE MS SQL SERVER 2016 SOBRE SERVIDORES WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA DEL ENS".

1. COMPROBACIONES EN CONTROLADOR DE DOMINIO

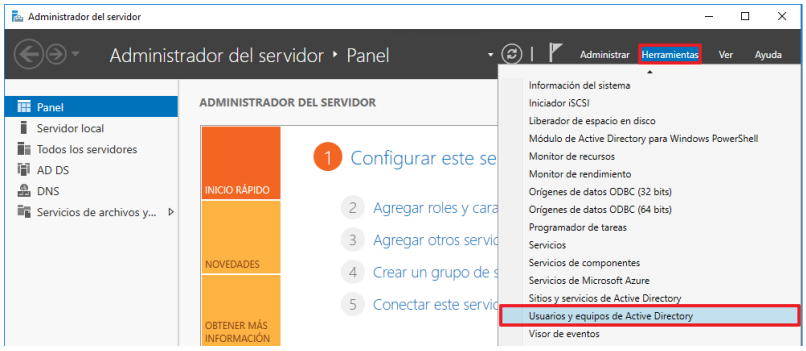
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador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

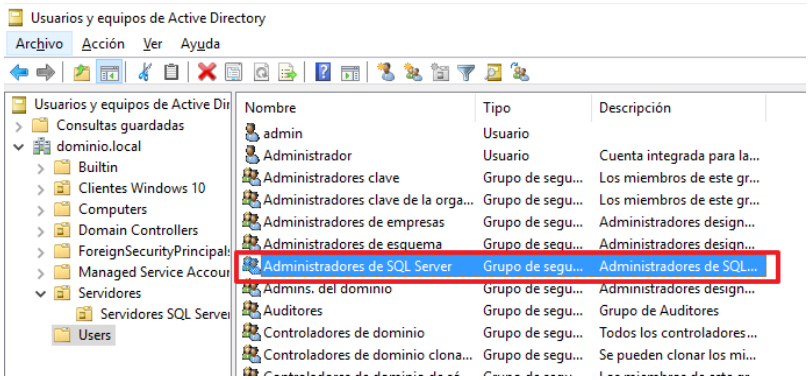
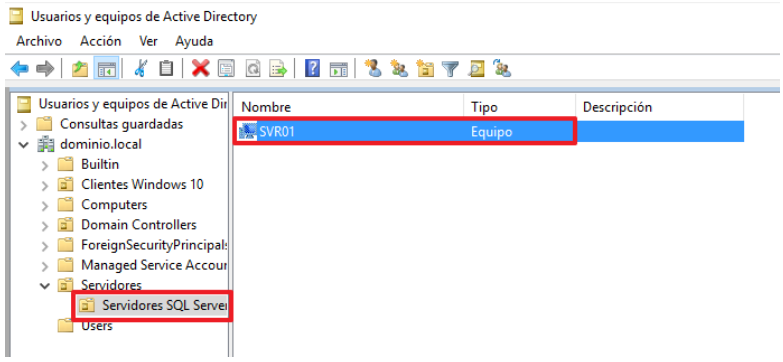
a) Usuarios y equipos de Active Directory (dsa.msc).

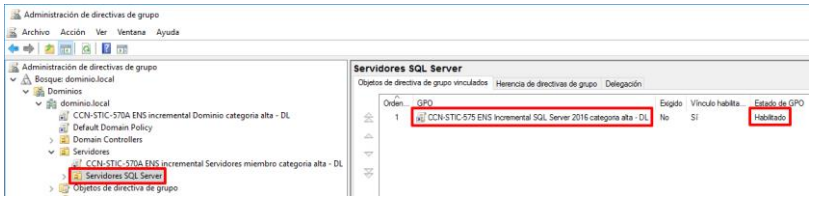
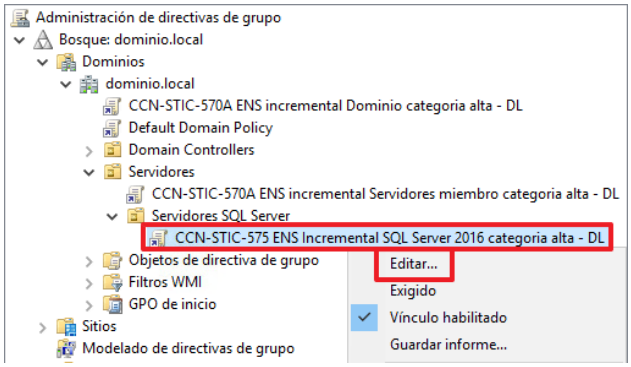
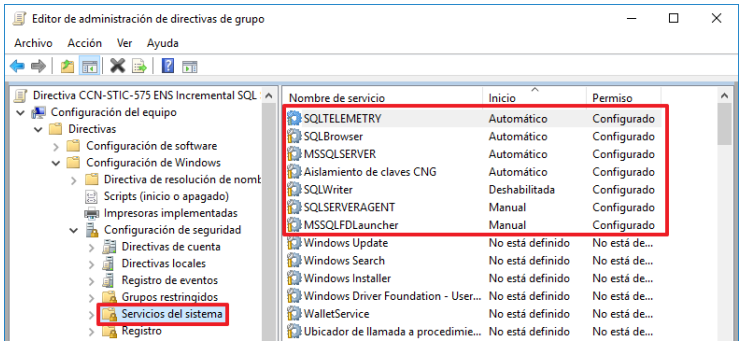
b) Administrador de directivas de grupo (gpmc.msc).

c) Editor de objetos de directiva de grupo (gpedit.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 el servidor controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
2. Verifique que está creado el grupo "Administradores de SQL Server" dentro del contenedor "Users".		Ejecute la herramienta "Usuarios y equipos de Active Directory". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Usuarios y equipos de Active Directory"** 

Comprobación	OK/NOK	Cómo hacerlo
		Seleccione el contenedor "Users", situado en la siguiente ruta: **"Usuarios y equipos de Active Directory → [Su dominio] → Users"** A continuación, en el panel de la derecha, verifique que está creado el objeto denominado "Administradores de SQL Server". 
3. Verifique que los servidores que tienen SQL Server instalado están dentro del contenedor "Servidores SQL Server".		Utilizando la misma consola de "Usuarios y Equipos de Directorio Activo" **(Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory).** Seleccione la unidad organizativa "**Servidores → Servidores SQL Server**", y verifique que existe un objeto de tipo "Equipo" que corresponde al servidor donde se ha instalado SQL Server 2016.  **Nota:** En este ejemplo se ha utilizado la cuenta de equipo SVR01. En su organización los nombres pueden variar.
4. Verifique que los objetos de directivas de grupo han sido creados y están habilitados.		Ejecute la herramienta "Administrador de directivas de grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"** 

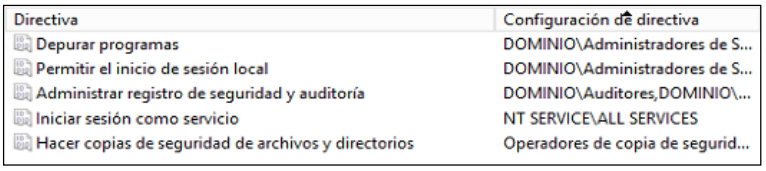
Comprobación	OK/NOK	Cómo hacerlo
		Dentro de la consola diríjase a los "Objetos de directiva de grupo": **"Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo"** Verifique que está creado el objeto de directiva de grupo "CCN-STIC-575 ENS Incremental SQL Server 2016 categoria alta - DL" y que en la columna "Estado de GPO" figura como habilitado.  **Nota:** En este ejemplo se ha utilizado la cuenta de equipo SVR01. En su organización los nombres pueden variar.
5. Verifique los servicios del sistema de la directiva SQL Server (CCN-STIC-575 Incremental SQL Server 2016 categoria alta - DL).		Seleccionando dicha directiva, pinche sobre ella con el botón derecho y seleccione la opción "Editar" del menú contextual, se abrirá la herramienta "Editor de administración de directiva de grupo" que permitirá verificar los valores de la directiva "CCN-STIC-575 ENS Incremental SQL Server 2016 categoria alta - DL".  Verifique que la directiva tiene los siguientes valores en servicios del sistema. Para ello, navegue hasta: **"Directiva CCN-STIC-575 ENS Incremental SQL Server 2016 categoria alta - DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del Sistema".** 

Comprobación	OK/NOK	Cómo hacerlo

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Aislamiento de claves CNG	KeyIso	Automático	Configurado	
SQL Server (MSQLSERVER)	MSSQLSERVER	Automático	Configurado	
SQL Server Browser	SQLBrowser	Automático	Configurado	
SQL Server CEIP service (MSSQLSERVER)	SQLTELEMETRY	Automático	Configurado	
SQL Server VSS Writer	SQLWriter	Deshabilitada	Configurado	
SQL Full-Text Filter Daemon Launcher	MSSQLFDLauncher	Manual	Configurado	
Agente SQL Server (MSSQLSERVER)	SQLSERVERAGENT	Manual	Configurado	

6. Verificación derechos de usuarios.

Utilizando el editor de directiva de grupo, verifique que la directiva "CCN-STIC-575 ENS Incremental SQL Server 2016 categoria alta - DL" tiene los siguientes valores en las directivas de asignación de derechos de usuario dentro de:
"Directiva → CCN-STIC-575 ENS Incremental SQL Server 2016 categoria alta - DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario".



Nota: Verifique que los permisos hayan quedado de la siguiente manera.

Directiva	Valor	OK/NOK
Administrar registro de seguridad y auditoría.	DOMINIO\Administradores de SQL Server, Administradores	
Depurar programas.	DOMINIO\Administradores de SQL Server	
Hacer copias de seguridad de archivos y directorios.	DOMINIO\Administradores de SQL Server, Administradores, Operadores de copia de seguridad	
Iniciar sesión como servicio.	NT SERVICE\ALL SERVICES	
Permitir el inicio de sesión local.	Administradores	

2. COMPROBACIONES EN EL SERVIDOR SQL SERVER 2016

Para realizar esta lista de comprobación primero deberá iniciar sesión en un servidor miembro de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

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

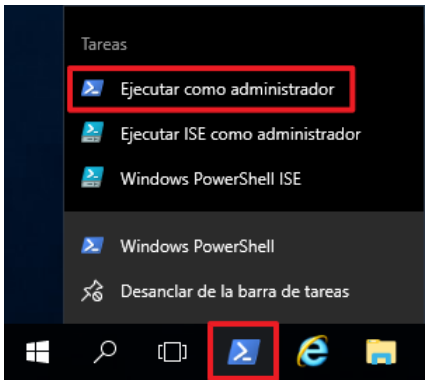
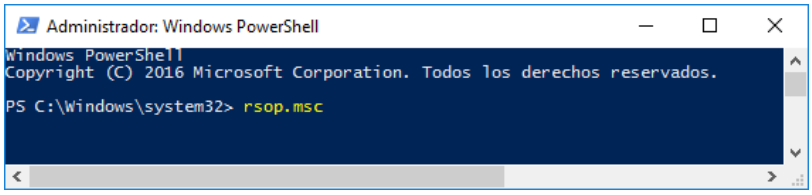
Las consolas y herramientas que se utilizarán son las siguientes:

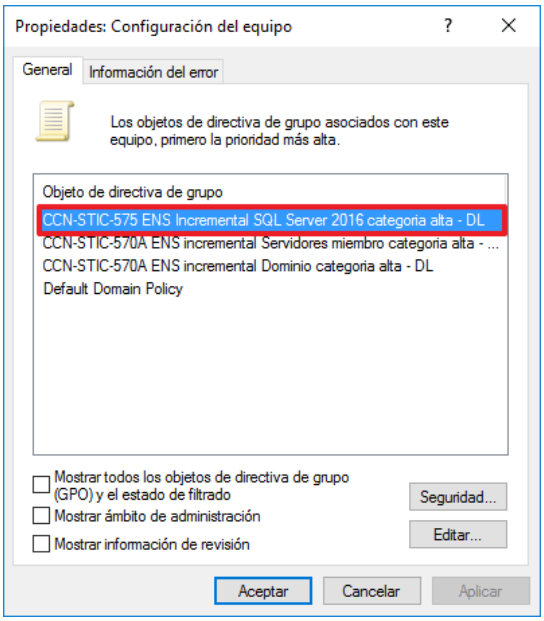
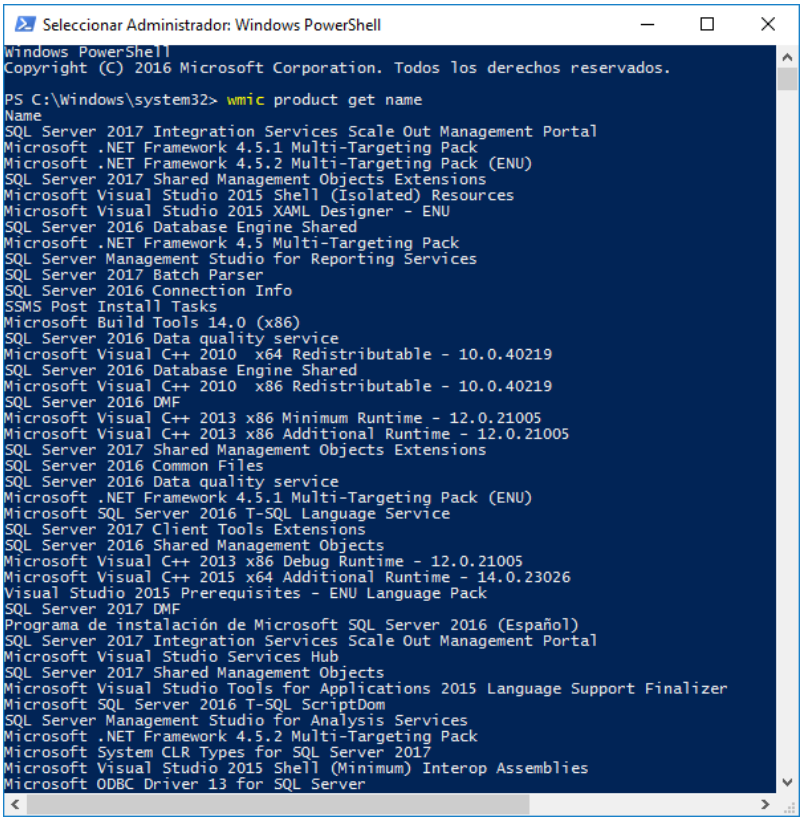
a) Conjunto resultante de directivas (rsop.msc).

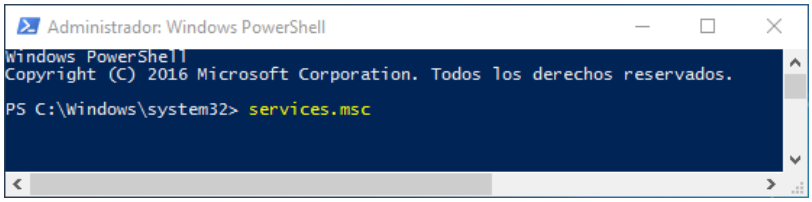
b) Servicios (services.msc).

c) Consola "SQL Server Management Studio".

d) Consola "Administrador de configuración de SQL Server".

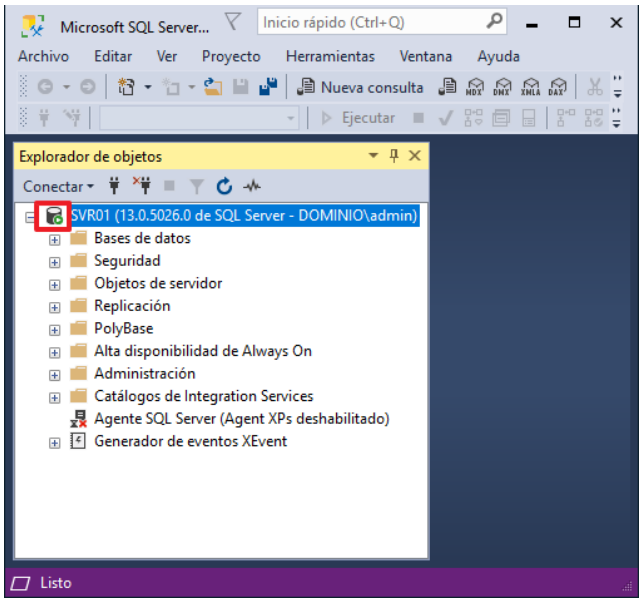
Comprobación	OK/NOK	Cómo hacerlo
7. Inicie sesión en el servidor de SQL Server 2016.		Inicie sesión en el servidor donde se ha implementado el servicio de Microsoft SQL Server 2016 con una cuenta que tenga privilegios de administración del dominio.
8. Verifique la correcta aplicación de la política "CCN-STIC-575 Incremental SQL Server 2016 categoria alta - DL" en un equipo miembro del dominio.		Ejecute una sesión de PowerShell como administrador. Para ello haga clic con el botón derecho sobre el icono de PowerShell de la barra de tareas, (ver la siguiente figura) y del menú contextual que aparecerá, marque la opción "Ejecutar como administrador", como se muestra en la imagen:  El "Control de cuentas de usuarios" le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse "Sí". Teclee rsop.msc en la consola de comandos que se ha abierto: 

Comprobación	OK/NOK	Cómo hacerlo
		A continuación, haga clic derecho sobre "Configuración de equipo" en la consola de "Conjunto resultante de directivas" y compruebe que la política "CCN-STIC-575 Incremental SQL Server 2016 categoria media" aparece en la lista como muestra la imagen. 
9. Verifique que SQL Server se ha instalado correctamente		Teclee "Wmic Product Get Name" en la consola de comandos que se ha abierto anteriormente, y compruebe que aparecen al menos los siguientes productos de SQL Server que se muestran en la siguiente imagen. 

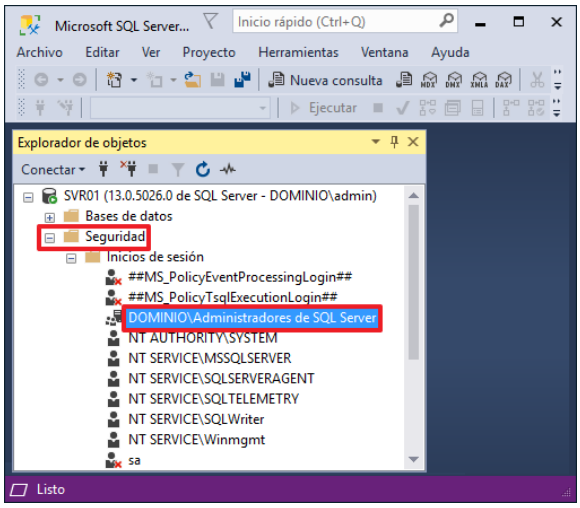
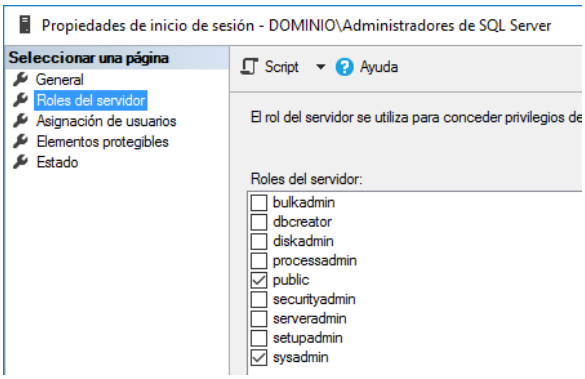
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>10. Verifique la correcta aplicación de la configuración de servicios del sistema de la política “CCN-STIC-575 Incremental SQL Server 2016 categoria alta - DL”.</td><td></td><td>Teclee “services.msc” en la consola de comandos que se ha abierto anteriormente:
 

En la consola de “Servicios”, compruebe los siguientes valores.</td></tr>
</table>

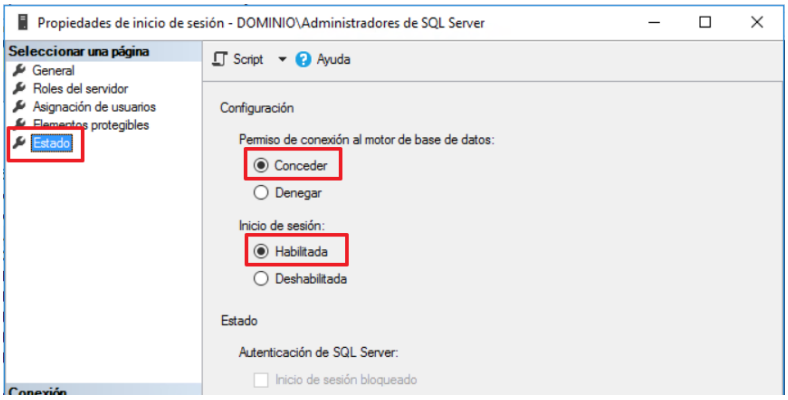
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Aislamiento de claves CNG	KeyIso	Automático	Configurado	
SQL Server (MSQLSERVER)	MSSQLSERVER	Automático	Configurado	
SQL Server Browser	SQLBrowser	Automático	Configurado	
SQL Server CEIP service (MSSQLSERVER)	SQLTELEMETRY	Automático	Configurado	
SQL Server VSS Writer	SQLWriter	Deshabilitada	Configurado	
SQL Full-Text Filter Daemon Launcher	MSSQLFDLauncher	Manual	Configurado	
Agente SQL Server (MSSQLSERVER)	SQLSERVERAGENT	Manual	Configurado	

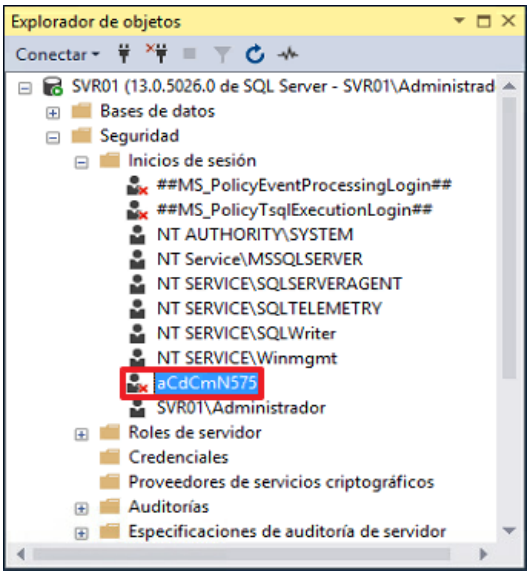
<table>
<tr><td>11. Verifique la correcta conexión con el servicio de SQL Server desde la consola de administración.</td><td></td><td>Utilizando la consola de administración de SQL Server Management 17 (“Inicio → Microsoft SQL Server Tools 17 → SQL Server Management Studio 17”).
Compruebe que se puede conectar correctamente al nombre del servidor que ejecuta el motor de bases de datos de SQL Server.
 

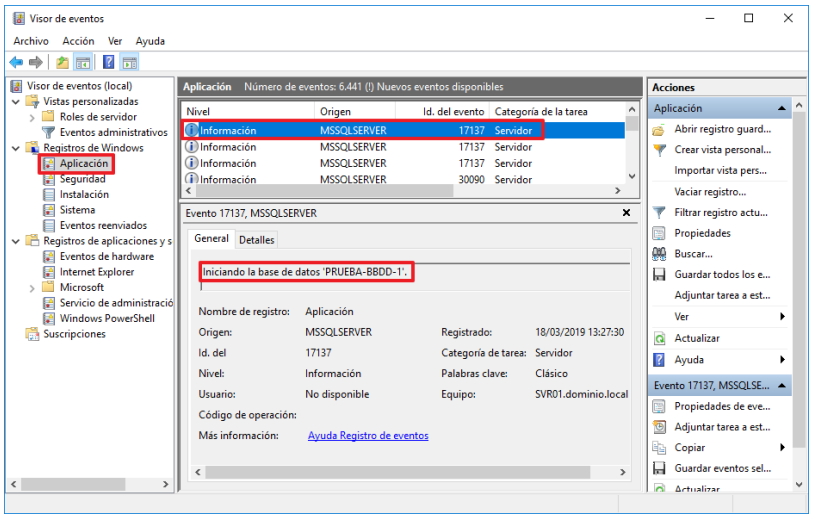
Nota: En este ejemplo se utiliza el nombre “SVR01.dominio.local”.</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>12. Verifique que el grupo de seguridad global “Administradores de SQL Server” está registrado en la consola de administración de SQL Server.</td><td></td><td>Utilizando la consola de administración de SQL 2016 (“Inicio → Microsoft SQL Server Tools 17 → SQL Server Management Studio 17”).
Compruebe que el grupo de dominio denominado “Administradores de SQL Server” esté configurado como inicio de sesión.
Navegue hasta el nodo “Seguridad → Inicio de sesión” y compruebe que existe el grupo “DOMINIO\Administradores de SQL Server”.
 
</td></tr>
<tr><td>13. Verifique los privilegios de roles del servidor para el grupo “Administradores de SQL Server”</td><td></td><td>Utilizando la consola de administración de SQL 2016 (Inicio → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17).
Verifique que el grupo de dominio denominado “Administradores de SQL Server” dispone de los permisos adecuados para administrar SQL Server.
Con el botón derecho seleccione el grupo “DOMINIO\Administradores de SQL Server” y haga clic en la opción del menú contextual “Propiedades”. A continuación, seleccione “Roles de servidor” y verifique que están habilitados los roles “Sysadmin” y “Public”.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Public</td><td>Habilitado</td><td></td></tr>
<tr><td>Sysadmin</td><td>Habilitado</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>14. Verifique el estado de las propiedades de inicio de sesión.</td><td></td><td>Utilizando la consola de administración de SQL 2016 (Inicio → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17).
Verifique que el grupo de dominio denominado “Administradores de SQL Server” tiene habilitado el inicio de sesión.
Con el botón derecho seleccione el grupo “DOMINIO\Administradores de SQL Server” y haga clic en la opción del menú contextual “Propiedades”. A continuación, seleccione “Estado” y verifique que el permiso de conexión al motor de base de datos esté concedido y que el inicio de sesión esté habilitado.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Permiso de conexión al motor de base de datos</td><td>Conceder</td><td></td></tr>
<tr><td>Inicio de sesión</td><td>Habilitado</td><td></td></tr>
</table></td></tr>
<tr><td>15. Verifique la conexión con el servicio de SQL Server desde la consola de administración.</td><td></td><td>Dentro del Explorador de archivos, despliegue el nodo “Servidor: <<nombre del servidor>> → Seguridad → Inicios de sesión” y compruebe que el usuario “sa”, previamente renombrado como “aCdCmN575”, se encuentra deshabilitado.
 
</td></tr>
</table>

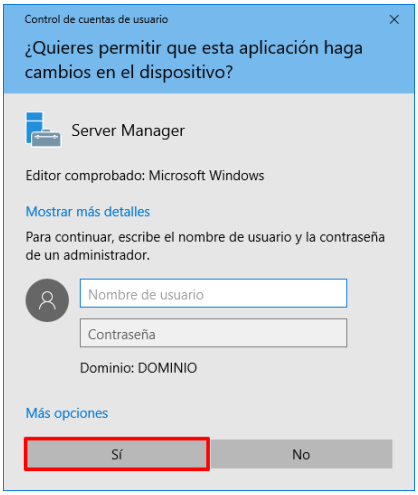
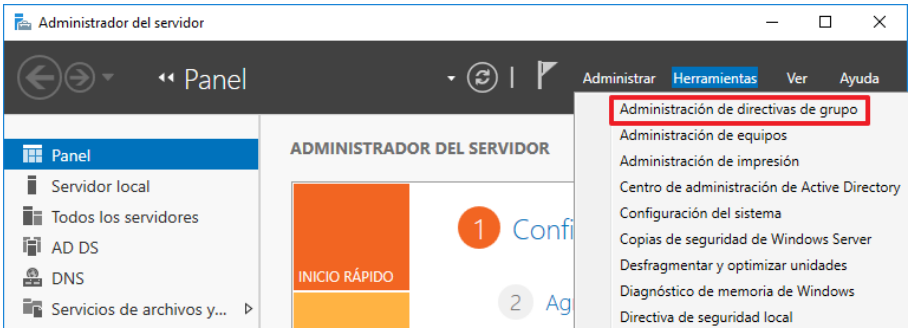
Comprobación	OK/NOK	Cómo hacerlo
16. Verifique que la auditoría sobre el servidor de SQL Server 2016 se encuentra activada.		Utilizando la herramienta de visor de eventos de Windows (ejecutando "eventvwr.msc" desde **Inicio → Ejecutar…)**, verifique que la auditoría del servidor del servidor de SQL Server 2016 se encuentra activada en el registro de "Aplicación". 

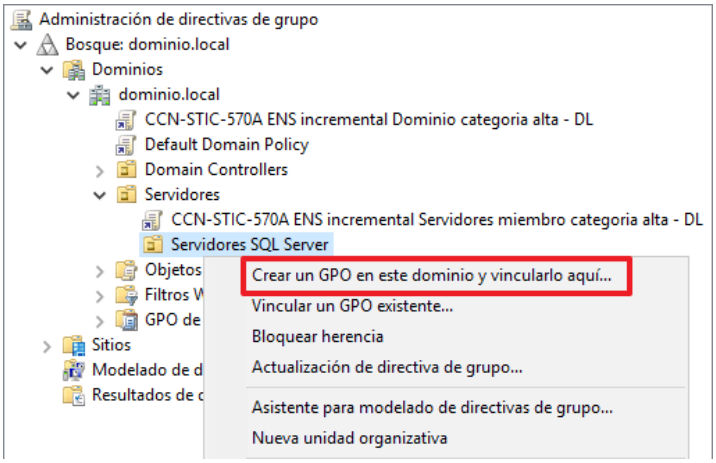
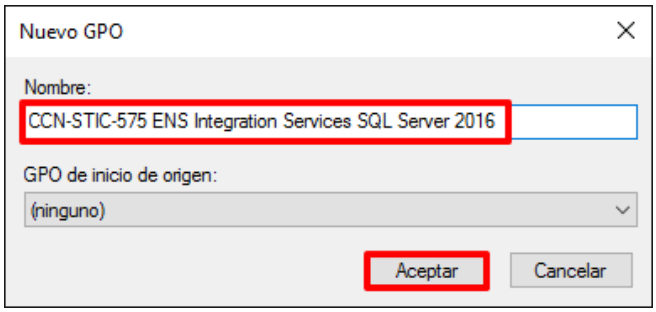
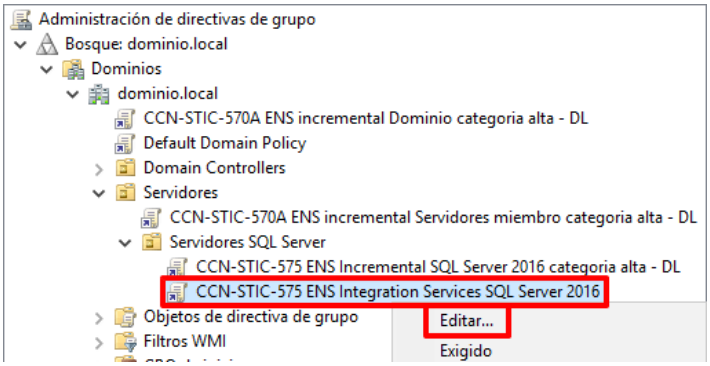
ANEXO A.5. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD

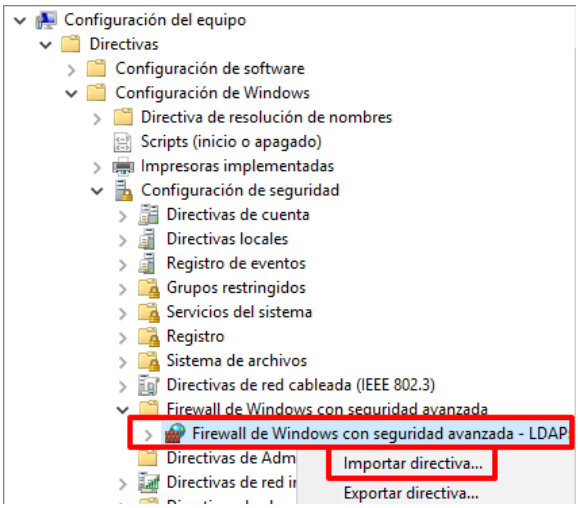
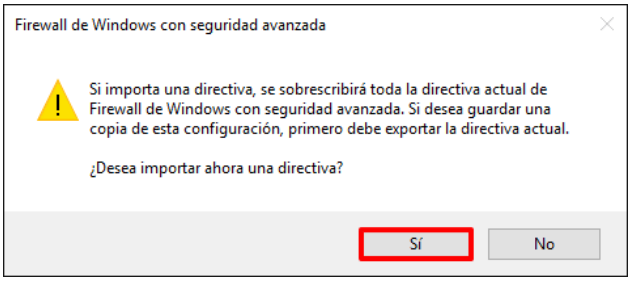
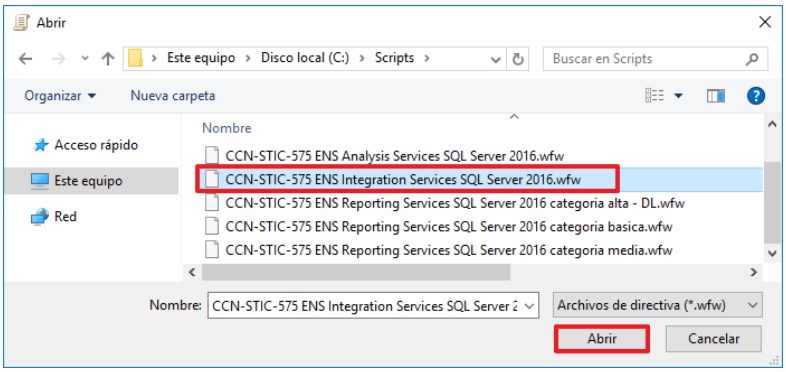
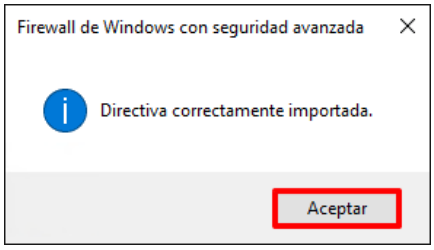
ANEXO A.5.1. ASIGNACIÓN DE PERMISOS SOBRE INTEGRATION SERVICES

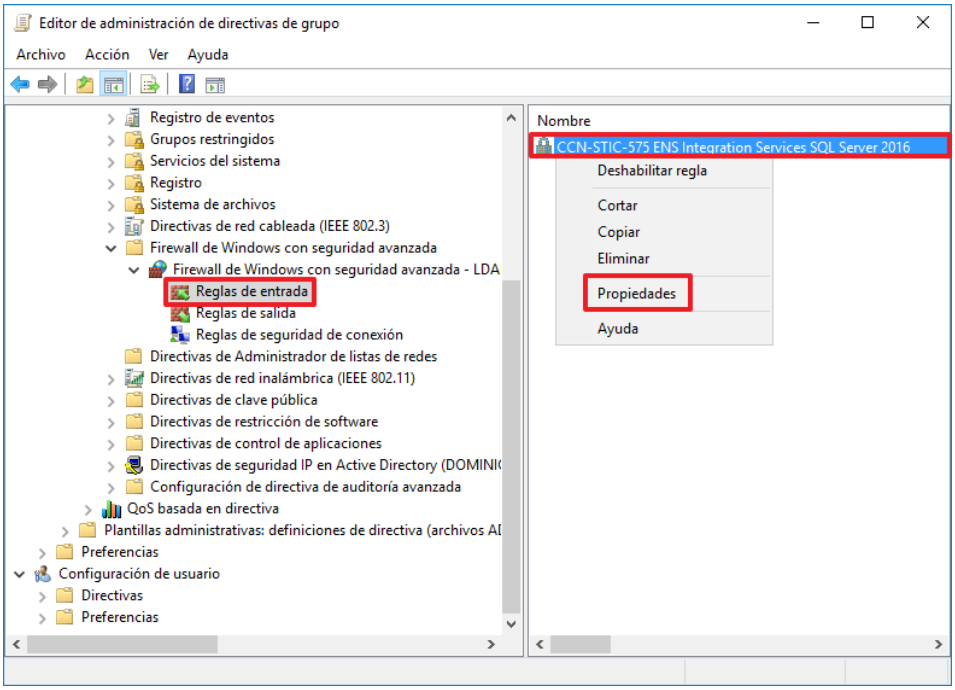
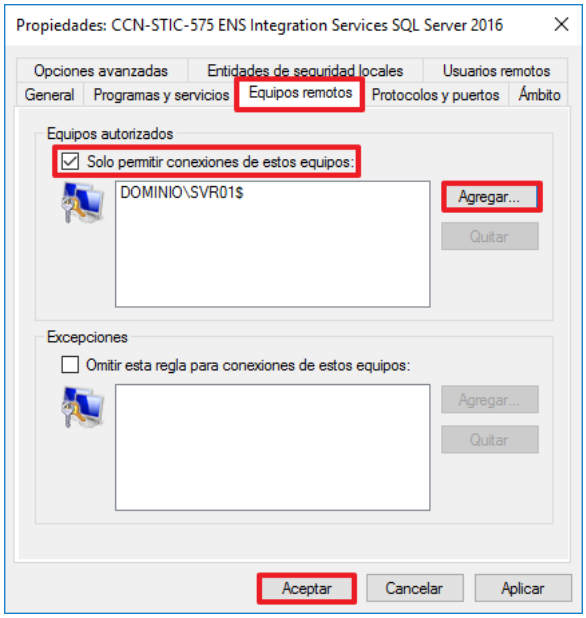
Si desea habilitar el uso de SQL Server Integration Services, deberá configurar los requisitos de configuración del firewall. En el siguiente apartado se muestran los pasos necesarios para poder habilitar la conexión de SQL Server Integration Services.

Nota: En los pasos descritos a continuación se establece una configuración de Integration Services válida para cualquier categoría del ENS.

Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor de SQL Server 2016. **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
2.	A continuación, abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
3.	El "Control de cuentas de usuarios" le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse "Sí". 
4.	En el "Administrador del servidor" despliegue el menú superior derecho "Herramientas" y a continuación seleccione "Administración de directivas de grupo". 

Paso	Descripción
5.	A continuación, despliegue el nodo "**Bosque: <<nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores SQL Server**". **Nota:** En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores se denomina "Servidores".
6.	Pulse con el botón derecho sobre "Servidores SQL Server" y haga clic sobre "Crear un GPO en este dominio y vincularlo aquí…". 
7.	A continuación, en el cuadro de diálogo, escriba el nombre de la GPO, "CCN-STIC-575 ENS Integration Services SQL Server 2016", y haga clic en el botón "Aceptar". 
8.	Edite la GPO recién creada en la unidad organizativa haciendo clic con el botón derecho en ella y seleccionando la opción "Editar". 
9.	Sitúese en el nodo "Configuración de seguridad", ubicado en **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad→ Firewall de Windows con seguridad Avanzada → Firewall de Windows con seguridad Avanzada – LDAP://[…]".**

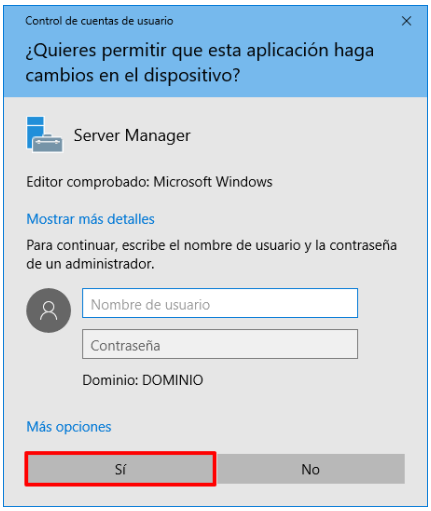
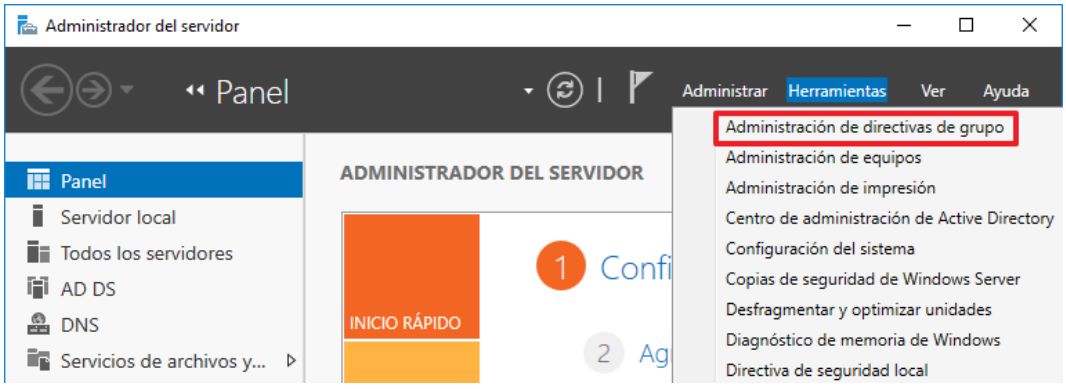
Paso	Descripción
10.	En la siguiente pantalla despliegue el árbol hasta el nodo Firewall de Windows y seleccione el nodo con el botón izquierdo de ratón, posteriormente pulse el botón derecho del ratón sobre la opción "Importar directiva…". 
11.	En la siguiente pantalla pulse el botón "Sí". 
12.	Sitúese en la carpeta "C:\Scripts" y seleccione el fichero denominado "CCN-STIC-575 ENS Integration Services SQL Server 2016.wfw", y pulse "Abrir". 
13.	Pulse "Aceptar" en la siguiente pantalla. 

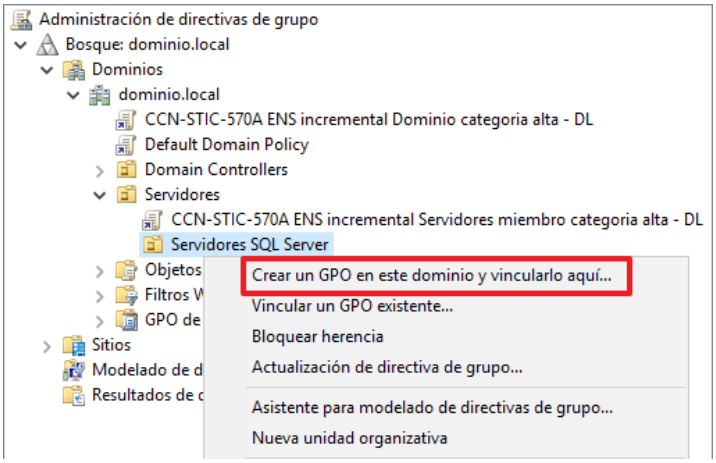
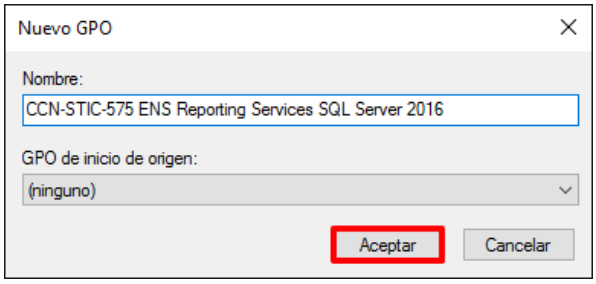
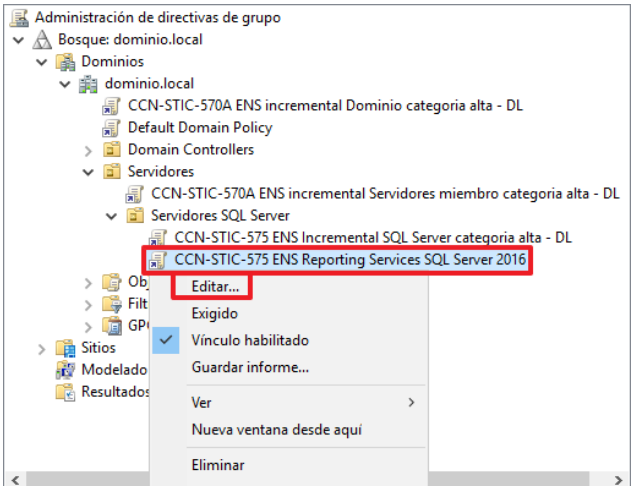
Paso	Descripción
14.	A continuación, dentro de "Reglas de entrada" seleccione la regla recién importada "CCN-STIC-575 ENS Integration Services SQL Server 2016" y haga clic con el botón derecho sobre ella y seleccione la opción "Propiedades". 
15.	Dentro de propiedades, diríjase a la pestaña "Equipos remotos" y marque la opción "Sólo permitir conexiones de estos equipos:". A continuación, pulse "Agregar" para añadir los equipos que desee. Pulse "Aceptar" para guardar los cambios.  **Nota:** En este ejemplo, se han habilitado los puertos para el equipo "DOMINIO\SVR01".

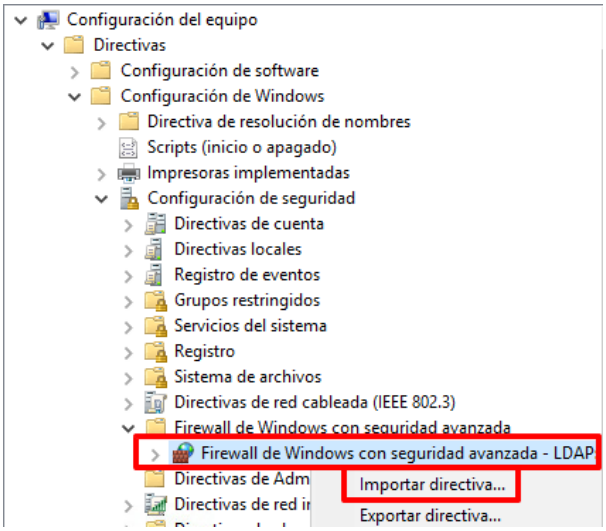
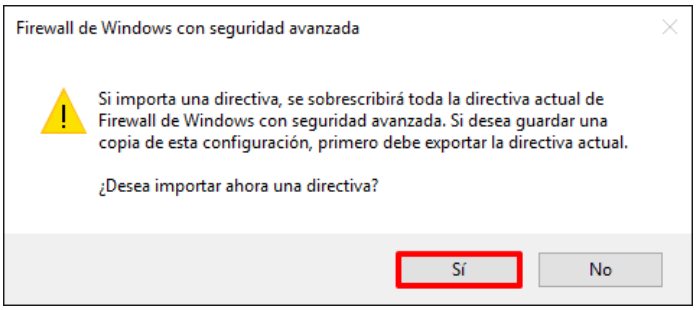
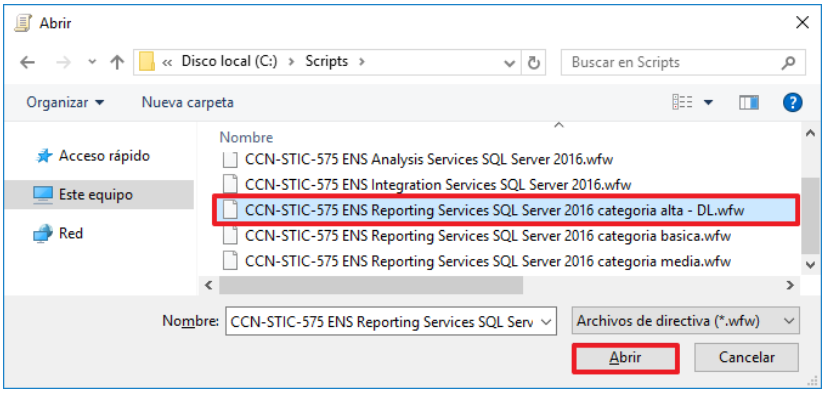
ANEXO A.5.2. ASIGNACIÓN DE PERMISOS SOBRE REPORTING SERVICES

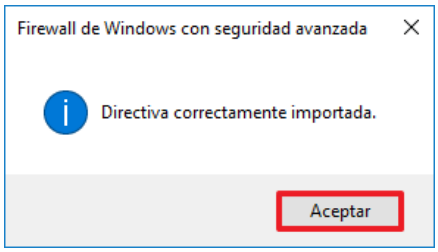
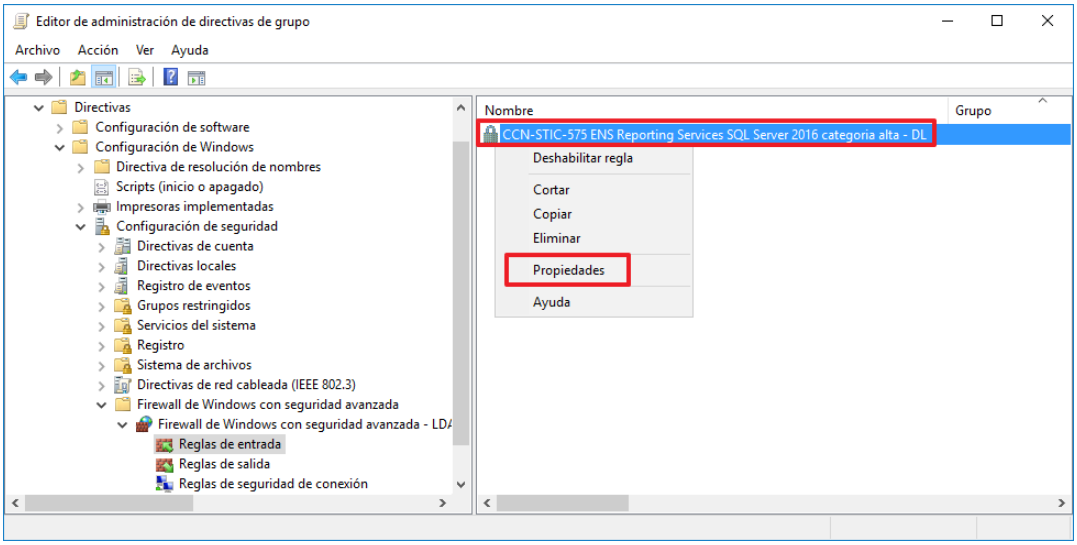
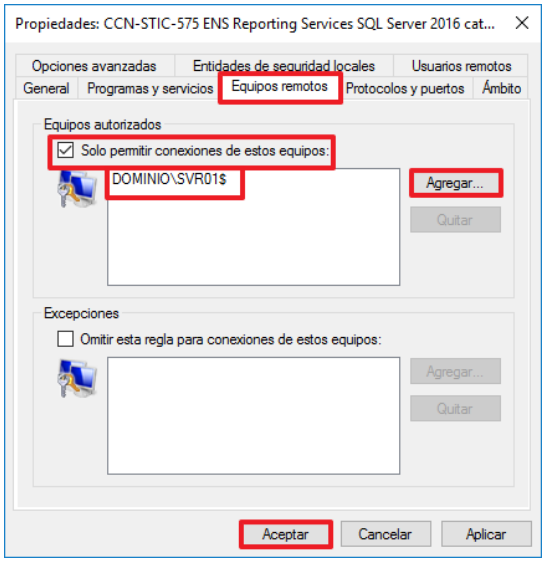
Si desea habilitar el uso de SQL Server Reporting Services, deberá configurar los requisitos de configuración del firewall. En el siguiente apartado se muestran los pasos necesarios para poder habilitar la conexión de SQL Server Reporting Services.

Nota: En los pasos descritos a continuación se establece una configuración de Reporting Services para un entorno de Categoría alta – DL. Deberá elegir la directiva de configuración de firewall acorde a la categoría de su organización.

Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor que se va a instalar. **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
2.	A continuación, abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
3.	El "Control de cuentas de usuarios" le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse "Sí". 
4.	En el "Administrador del servidor" despliegue el menú superior derecho "Herramientas" y a continuación seleccione "Administración de directivas de grupo". 

Paso	Descripción
5.	A continuación, despliegue el nodo "**Bosque: <<nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores SQL Server**". **Nota:** En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores se denomina "Servidores".
6.	Pulse con el botón derecho sobre "Servidores SQL Server" y haga clic sobre "Crear un GPO en este dominio y vincularlo aquí…". 
7.	A continuación, en el cuadro de diálogo, escriba el nombre de la GPO, "CCN-STIC-575 ENS Reporting Services SQL Server 2016" y pulsar el botón "Aceptar". 
8.	Edite la GPO recién creada en la unidad organizativa haciendo clic con el botón derecho en ella y seleccionando la opción "Editar". 

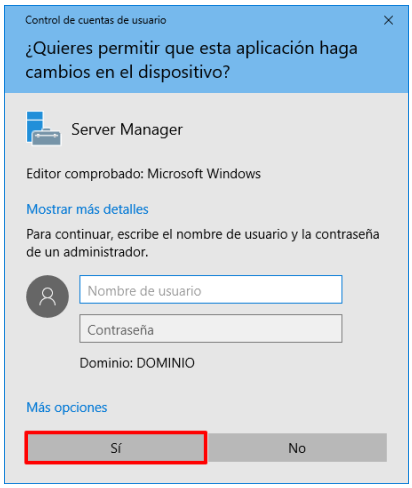
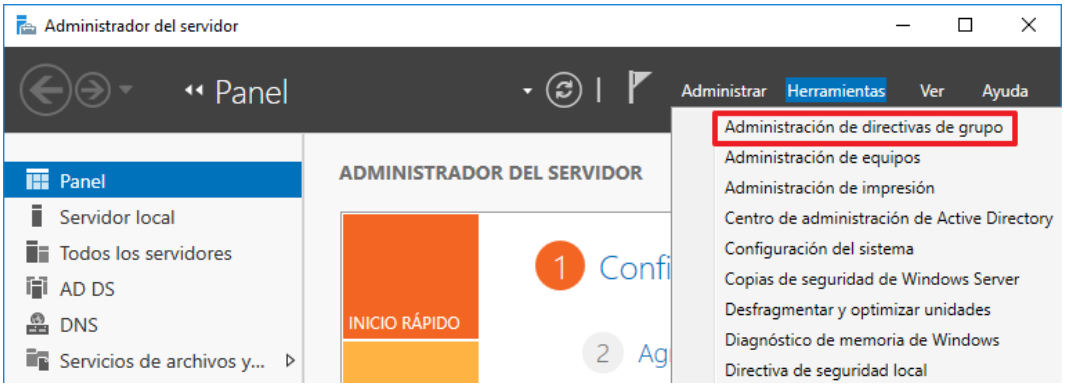
Paso	Descripción
9.	Sitúese en el nodo "Configuración de seguridad", ubicado en **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad→ Firewall de Windows con seguridad Avanzada → Firewall de Windows con seguridad Avanzada – LDAP://[…]".**
10.	En la siguiente pantalla despliegue el árbol hasta el nodo Firewall de Windows y seleccione el nodo con el botón izquierdo de ratón, posteriormente pulse el botón derecho del ratón sobre la opción "Importar directiva…". 
11.	En la siguiente pantalla pulse el botón "Sí". 
12.	Sitúese en la carpeta "C:\Scripts" y busque el fichero de configuración de firewall acorde a la categoría de su organización. En un entorno de categoría alta – DL seleccione el fichero "CCN-STIC-575 ENS Reporting Services SQL Server 2016 categoria alta - DL.wfw" y pulse "Abrir". 

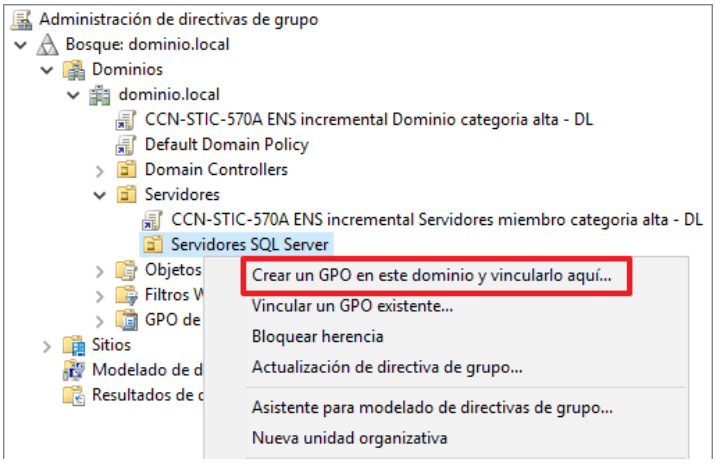
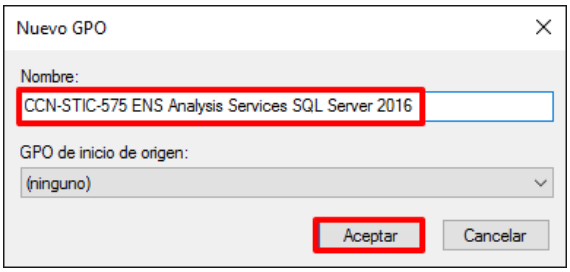
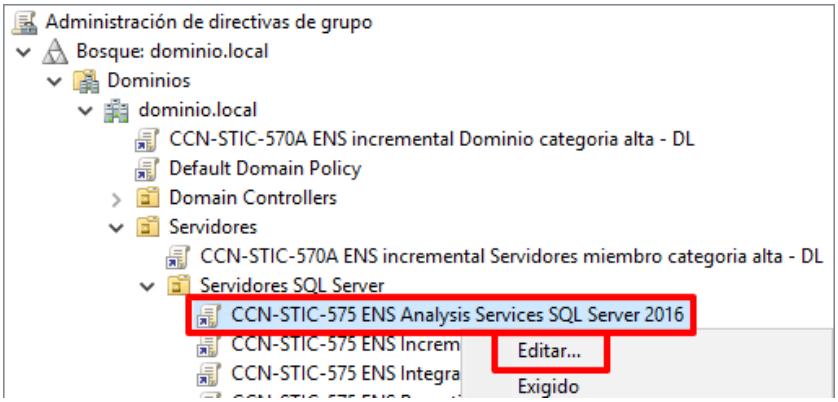
Paso	Descripción
13.	Pulse "Aceptar" en la siguiente pantalla. 
14.	A continuación, dentro de "Reglas de entrada" seleccione la regla recién importada "CCN-STIC-575 ENS Reporting Services SQL Server 2016 categoria alta - DL" y haga clic con el botón derecho sobre ella y seleccione la opción "Propiedades". 
15.	Seleccione la pestaña "Equipos remotos", marque la opción "Sólo permitir conexiones de estos equipos:" y en el cuadro de Equipos autorizados" añada su servidor mediante el botón "Agregar". Finalmente, pulse "Aceptar".  **Nota:** En este ejemplo, se han habilitado los puertos para el equipo "DOMINIO\SVR01".

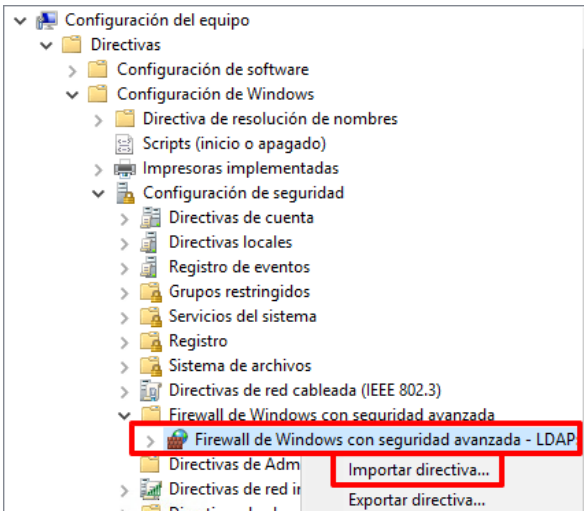
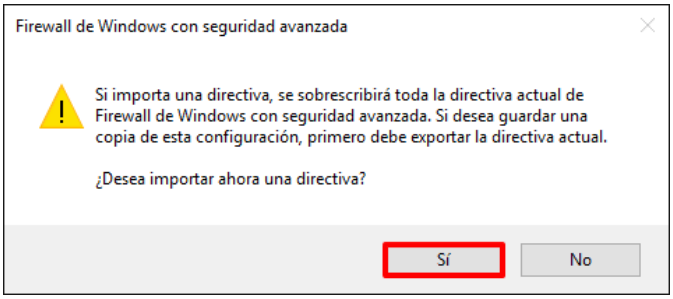
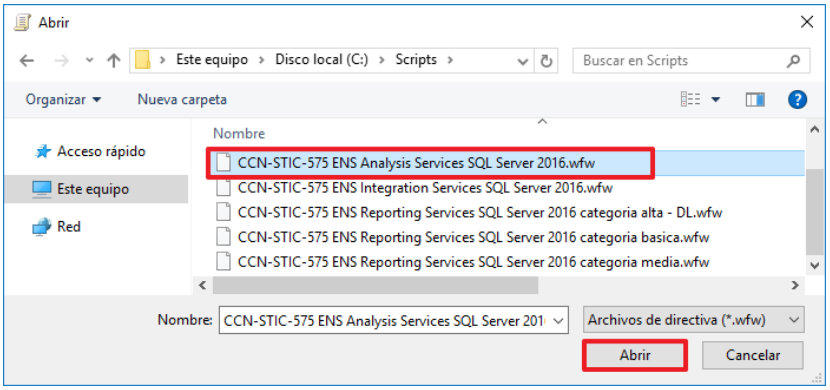
ANEXO A.5.3. ASIGNACIÓN DE PERMISOS SOBRE ANALYSIS SERVICES

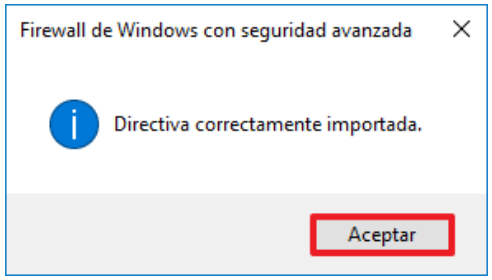
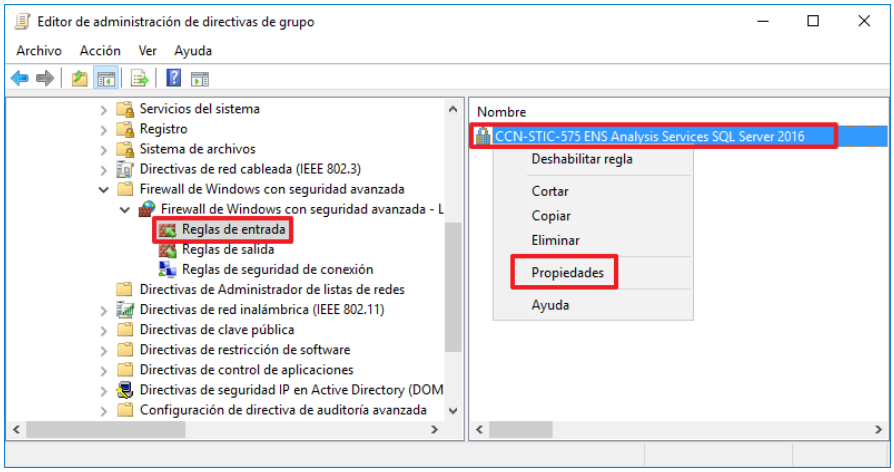
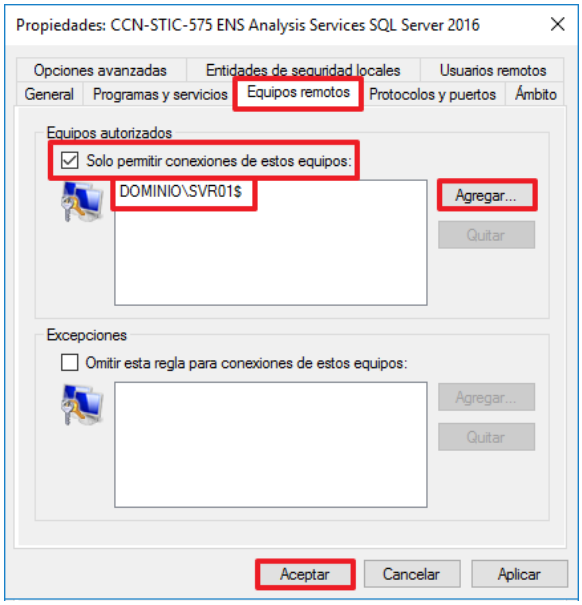
Si desea habilitar el uso de SQL Server Analysis Services, deberá configurar los requisitos de configuración del firewall. En el siguiente apartado se muestran los pasos necesarios para poder habilitar la conexión de SQL Server Analysis Services.

Nota: En los pasos descritos a continuación se establece una configuración de Analysis Services válida para cualquier categoría del ENS.

Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio del dominio al que pertenece el servidor de SQL Server 2016. **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
2.	A continuación, abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
3.	El "Control de cuentas de usuarios" le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse "Sí". 
4.	En el "Administrador del servidor" despliegue el menú superior derecho "Herramientas" y a continuación seleccione "Administración de directivas de grupo". 

Paso	Descripción
5.	A continuación, despliegue el nodo "**Bosque: <<nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores SQL Server**". **Nota:** En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores se denomina "Servidores".
6.	Pulse con el botón derecho sobre "Servidores SQL Server" y haga clic sobre "Crear un GPO en este dominio y vincularlo aquí…". 
7.	A continuación, en el cuadro de diálogo, escriba el nombre de la GPO, "CCN-STIC-575 ENS Analysis Services SQL Server 2016", y haga clic en el botón "Aceptar". 
8.	Edite la GPO recién creada en la unidad organizativa haciendo clic con el botón derecho en ella y seleccionando la opción "Editar". 
9.	Sitúese en el nodo "Configuración de seguridad", ubicado en **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad→ Firewall de Windows con seguridad Avanzada → Firewall de Windows con seguridad Avanzada – LDAP://[…]".**

Paso	Descripción
10.	En la siguiente pantalla despliegue el árbol hasta el nodo Firewall de Windows y seleccione el nodo con el botón izquierdo de ratón, posteriormente pulse el botón derecho del ratón sobre la opción "Importar directiva...". 
11.	En la siguiente pantalla pulse el botón "Sí". 
12.	Sitúese en la carpeta "C:\Scripts" y seleccione el fichero denominado "CCN-STIC-575 ENS Analysis Services SQL Server 2016.wfw", seguidamente pulse el botón "Abrir". 

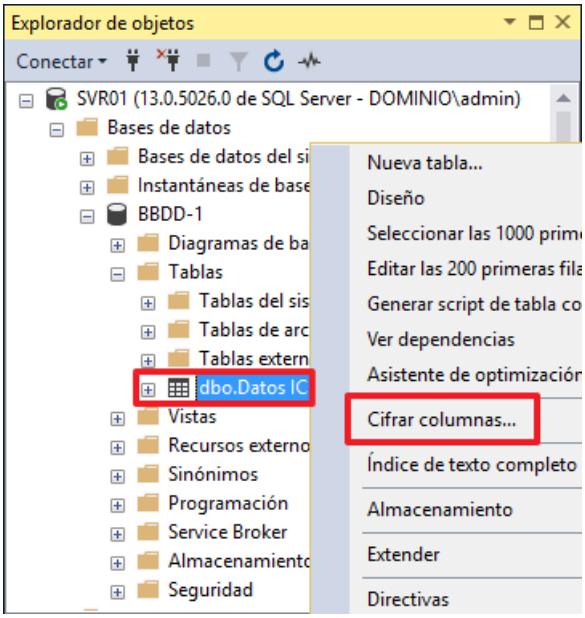
Paso	Descripción
13.	Pulse "Aceptar" en la siguiente pantalla. 
14.	A continuación, dentro de "Reglas de entrada" seleccione la regla recién importada "CCN-STIC-575 ENS Integration Services SQL Server 2016" y haga clic con el botón derecho sobre ella y seleccione la opción "Propiedades". 
15.	Seleccione la pestaña "Equipos remotos", marque la opción "Sólo permitir conexiones de estos equipos:" y en el cuadro de "Equipos autorizados" añada su servidor mediante el botón "Agregar". Finalmente, pulse "Aceptar".  **Nota:** En este ejemplo, se han habilitado los puertos para el equipo "DOMINIO\SVR01".

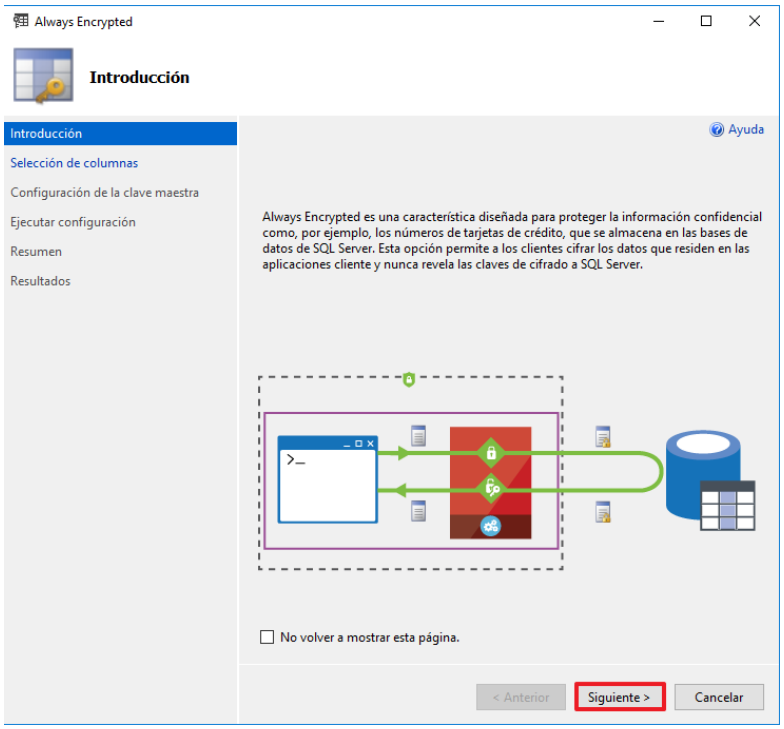
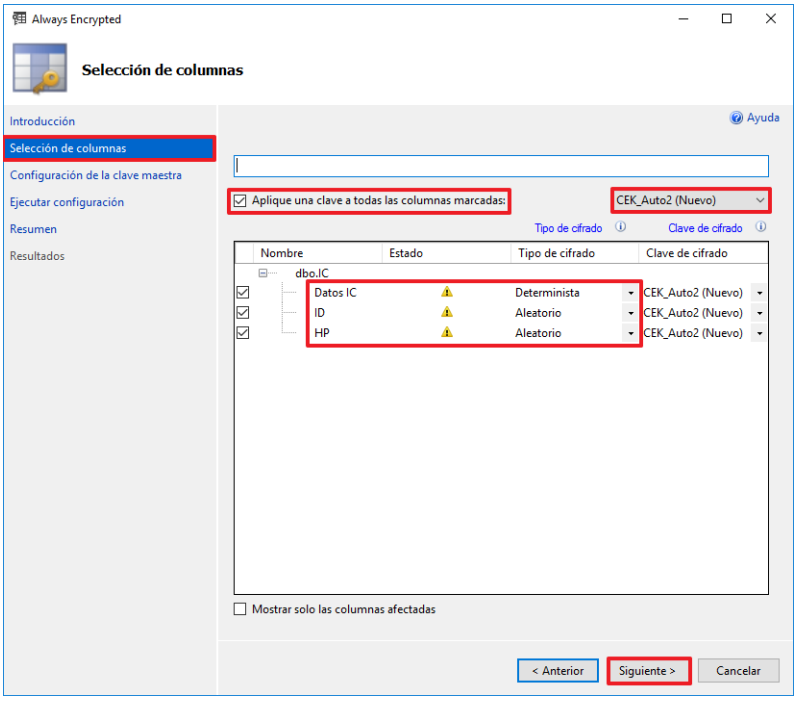
ANEXO A.5.4. CIFRADO DE ELEMENTOS DE SQL SERVER 2016

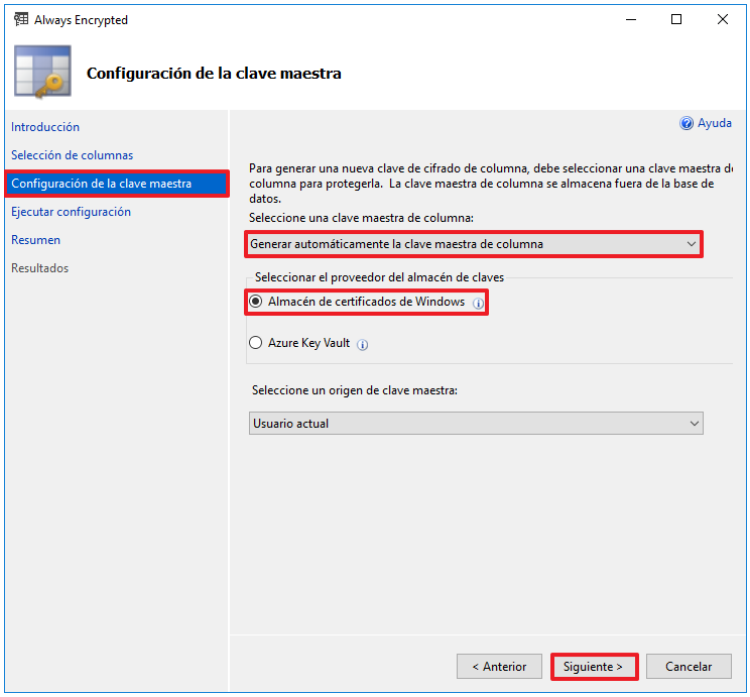
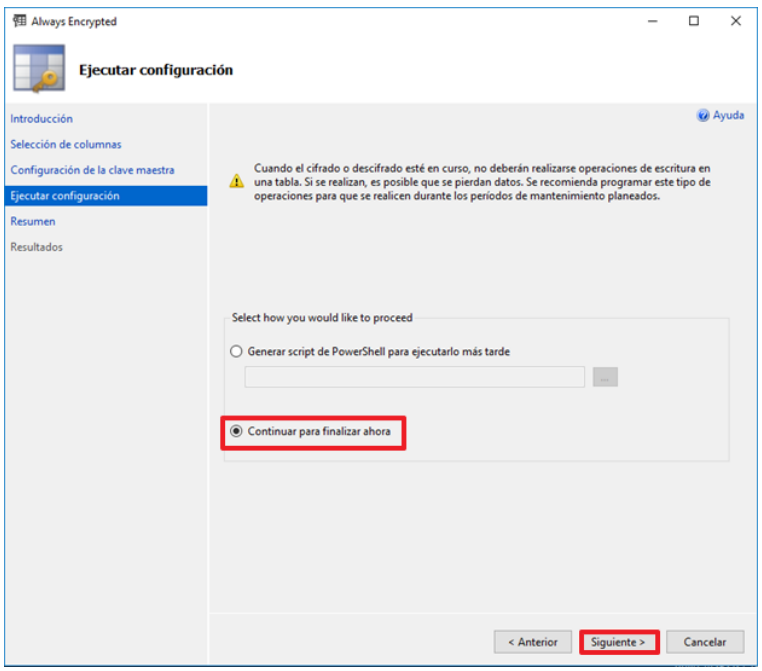
SQL Server 2016 ofrece la posibilidad de cifrar sus las tablas de sus bases de datos mediante la característica Always Encrypted que usa dos tipos de claves: clave maestra de columna y clave de cifrado de columna. Una clave maestra de columna (CMK) es una clave de cifrado de claves, que se encuentra siempre bajo el control del cliente y se almacena en un almacén de claves externo. Una clave de cifrado de columna (CEK) es una clave de cifrado de contenido que está protegida por una CMK.

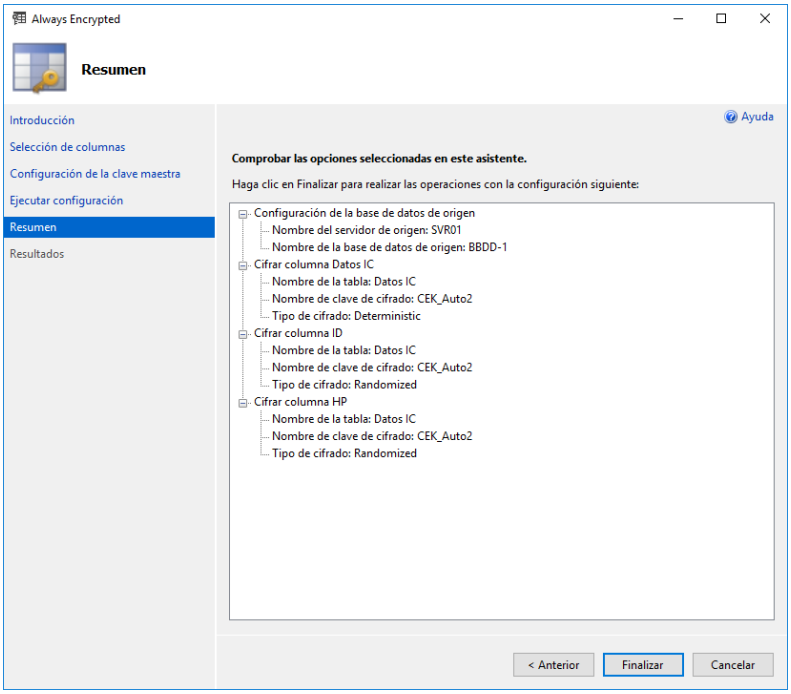
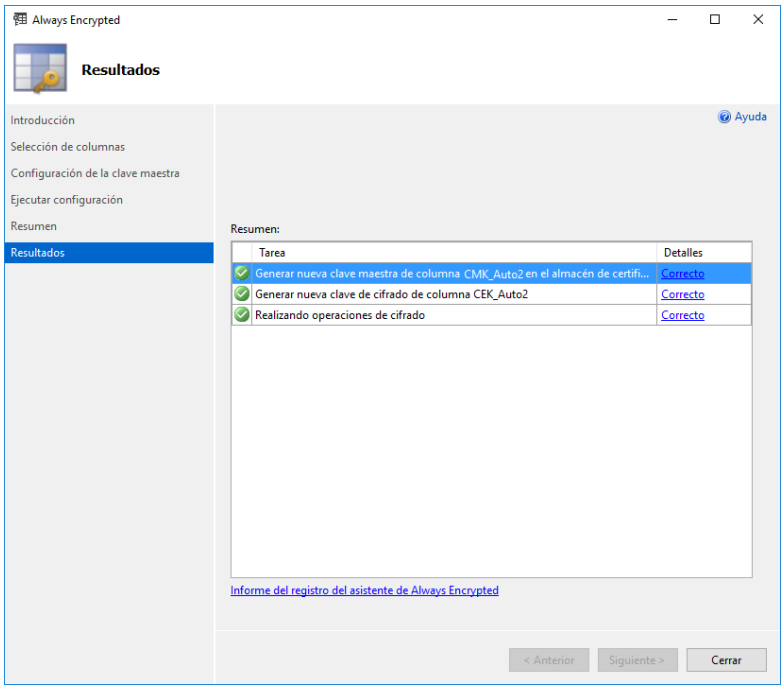
Always Encrypted usa el algoritmo AEAD_AES_256_CBC_HMAC_SHA_256 para cifrar los datos de la base de datos, ya que a excepción de AES_128, AES_192 y AES_256 todos los algoritmos se encuentran en desuso.

En el apartado se muestran las configuraciones necesarios para poder cifrar una tabla utilizando Always Encrypted como método de cifrado.

Paso	Descripción
1.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
2.	Inicie el administrador de SQL Server 2017 Management Studio desde **"Inicio → Herramientas administrativas → Microsoft SQL Server Tools 17 → Microsoft SQL Server Management Studio 17"**.
3.	En la ventana de "Conectar con el servidor", asegúrese que el nombre del servidor es el correcto y pulse "Conectar".
4.	A continuación, despliegue el nodo **"Servidor: <<nombre del servidor>> → Base de datos <<nombre de base de datos>> → Tablas → Tabla <<nombre de tabla>>"** y desplegando el menú contextual con el botón derecho, seleccione la opción "Cifrar columnas…".  **Nota:** En este ejemplo, se utiliza la tabla "Datos IC".

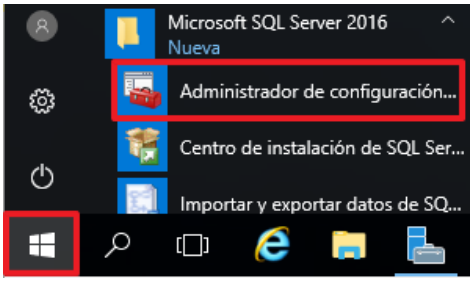
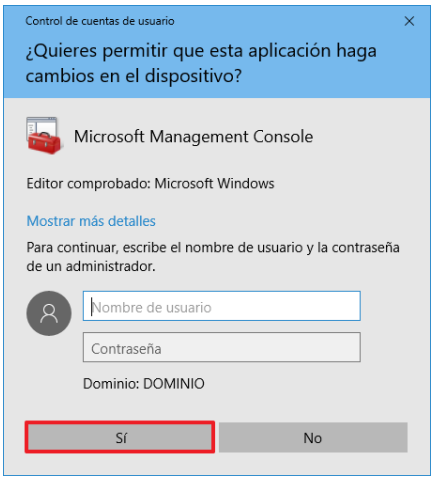
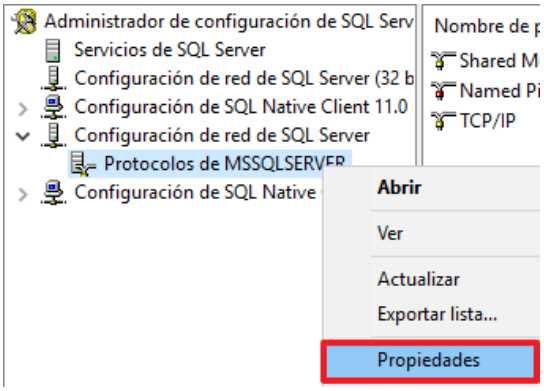
Paso	Descripción
5.	En la siguiente ventana de Always Encrypted pulse "Siguiente >" para continuar. 
6.	En la pantalla de "Selección de columnas", podrá elegir las columnas que desea cifrar. Para ello, marque la casilla "Aplique una clave a todas las columnas marcadas y elija una nueva clave de cifrado. Establezca un tipo de cifrado "Aleatorio" para todas las columnas. Pulse "Siguiente>" cuando haya finalizado.  **Nota:** Tenga en consideración que no puede utilizar un tipo de cifrado aleatorio sobre una columna establecida como clave principal.

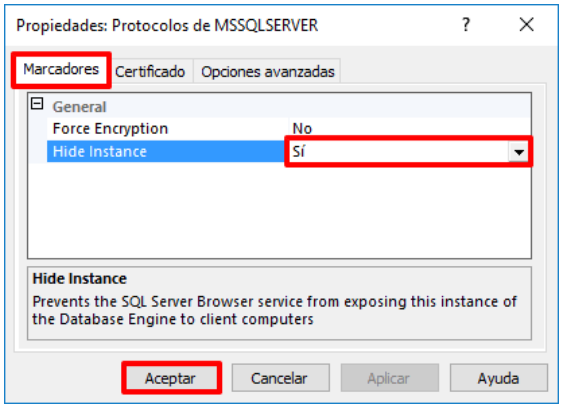
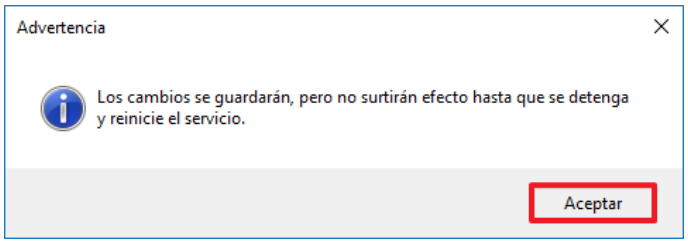
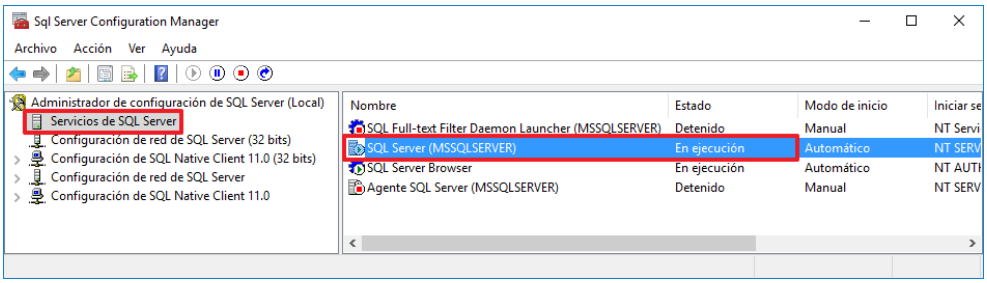
Paso	Descripción
7.	Ahora, configure la clave maestra, para ello seleccione "Generar automáticamente la clave maestra de columna y marque la opción de guardar en el "Almacén de certificados Windows".  **Nota:** Las claves maestra de columna y cifrado de columna se almacenan en la base de datos de la tabla que este cifrando.
8.	En la siguiente pantalla, marque la opción "Continuar para finalizar ahora" y pulse "Siguiente >". 

Paso	Descripción
9.	Pulse "Finalizar" en la siguiente ventana. 
10.	Para finalizar el proceso de cifrado, pulse el botón "Cerrar".  **Nota:** Tenga en consideración si tiene habilitada una auditoria sobre la tabla que desea cifrar, no podrá realizar la operación de cifrado con éxito.

ANEXO A.5.5. OCULTAR INSTANCIA DEL MOTOR DE BASE DE DATOS

Para ocultar una instancia del motor de base de datos de SQL Server siga los siguientes pasos.

Paso	Descripción
1.	Inicie sesión en el servidor miembro del dominio donde se ha implementado Microsoft SQL Server 2016. **Nota:** Inicie sesión con una cuenta con privilegios de administración.
2.	Inicie el administrador de Administrador de configuración de SQL Server 2016 desde **"Inicio → Herramientas administrativas → Microsoft SQL Server 2016 → Administración de configuración".** 
3.	El "Control de cuentas de usuarios" le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador de dominio y pulse "Sí". 
4.	En la consola de administración sitúese sobre el nodo **"Configuración de red de SQL Server → Protocolos [Instancia Servidor]"** haga clic con el botón derecho y seleccione la opción "Propiedades". 

Paso	Descripción
5.	En la pestaña "Marcadores", establezca el valor del campo "Hide Instance" en "Sí". A continuación, haga clic en "Aceptar" para cerrar el cuadro de diálogo.  **Nota:** Si oculta una instancia, deberá proporcionar el número de puerto en la cadena de conexión para conectarse a la instancia oculta. Se recomienda utilizar un puerto estático en lugar de un puerto dinámico para la instancia con nombre oculta.
6.	El sistema alerta de que los cambios se guardaran, pero que no sufrirán efecto hasta que se detenta y reinicie el servicio. Pulse sobre el botón "Aceptar". 
7.	Sitúese en el nodo "Servicios de SQL Server" en la consola del Administrador de configuración de SQL Server y localice el servicio SQL Server (MSSQLSERVER). 
8.	Haga clic con el botón derecho sobre él y seleccione la opción "reiniciar" para detener e iniciar el servicio con la nueva configuración.