centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 576

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

JUNIO 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: 083-19-187-4
Fecha de Edición: junio de 2019

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

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

PRÓLOGO

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

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

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

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

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

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

junio de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE EXCHANGE SERVER 2016 SOBRE MICROSOFT WINDOWS SERVER 2016 EN EL ENS

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

1. APLICACIÓN DE MEDIDAS EN EXCHANGE SERVER 2016

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación de Exchange 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 Exchange 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 Exchange 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 las categorías que mecanismos se deberán habilitar para su cumplimiento. Habida cuenta de esta información a continuación se detallarán las diferentes plantillas de seguridad aplicables en función de las diferentes categorías de seguridad.

1.1. MARCO OPERACIONAL

1.1.1. CONTROL DE ACCESO

El control de acceso cubre todo el conjunto de acciones que bien preparatorias o ejecutivas orientadas a determinar qué o quién puede o no acceder a un recurso del sistema, mediante una determinada acción. Con el cumplimiento de todas las medidas se garantizará que nadie accederá a recursos sin la debida autorización. Adicionalmente se 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. 1. IDENTIFICACIÓN

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

Las limitaciones de acceso a los servicios web se establecerán basándose en los métodos de identificación disponibles según el contenido web al que se quiera acceder.

Debe tenerse en consideración que los requisitos para la identificación en un servidor IIS 10 serán gradualmente incrementados en cuanto a su robustez, según se eleve el nivel de seguridad en función de la categoría establecida por el ENS.

La implementación de uno u otro mecanismo de identificación que aporta IIS 10, vendrá también demandado por el tipo de sitio web que aloja el sistema sobre el que se pretende aplicar seguridad. Así una plataforma web de acceso público, demandará un sistema de autenticación anónima, aun siendo la categoría alta. No obstante, si esta misma plataforma contara con un espacio de acceso restringido para determinados usuarios, se implementará un mecanismo de autenticación asociado a la categoría requerida en el ENS.

Dentro de las guías de paso a paso se sugerirán los mecanismos de identificación más adecuados a cada una de las categorías de seguridad contempladas por el ENS.

La identificación de cada usuario se traduce en la necesidad de crear cuentas con un identificador único e inequívoco para cada usuario y servicio.

Nunca deberán existir dos cuentas iguales, de forma que éstas no puedan confundirse o bien imputarse acciones a usuarios diferentes al que haya realizado la acción a auditar.

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

Microsoft Exchange Server 2016, incluye una amplia variedad de permisos predefinidos, basados en el modelo de permisos de control de acceso basado en roles (RBAC). Los permisos que se conceden a los administradores y a los usuarios se basan en roles de administración.

Un rol o función define el conjunto de tareas que un administrador o un usuario pueden realizar. Por ejemplo, un rol de administración denominado "Mail Recipients" puede define las tareas que alguien puede realizar en un conjunto de buzones de correo, contactos y grupos de distribución. Cuando un rol se asigna a un administrador o usuario, a dicha persona se conceden los permisos que proporciona el rol en cuestión.

En Exchange Server 2016 existen grupos de roles predeterminados las cuales establecen las diferentes funciones a realizar en la administración de Exchange Server 2016.

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

IIS 10 se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso.

Exchange Server 2016 se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso. 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.

1.1.1.4. OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN

Exchange Server 2016 usará siempre la autenticación basada en usuarios de Active Directory prevaleciendo la configuración de seguridad establecida mediante las políticas de seguridad según se establece en el Esquema Nacional de Seguridad.

El servidor de acceso de clientes únicamente proporciona acceso para usuarios con los protocolos de acceso de clientes habituales: HTTP, POP e IMAP y SMTP.

El sistema de autenticación se puede traducir tecnológicamente mediante múltiples mecanismos, siendo el del empleo de usuario y contraseña el más habitual pero no por ello el más seguro, sino todo lo contrario. Los mecanismos de autenticación se deberán adecuar en función del nivel de criticidad de la información 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.

1.1.1.5. 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.

Exchange Server 2016, al igual que ya lo hacían sus predecesores proporciona mecanismos avanzados de seguridad para proteger las conexiones procedentes de fuentes no confiables como es Internet.

Dichos mecanismos implementan diferentes modelos de autenticación por certificados, dependiendo de si los extremos forman parte del mismo dominio, forman parte de dominios diferentes o son sistemas diferentes a Exchange.

La seguridad de nivel de transporte (TLS), es un protocolo estándar que se usa para proporcionar comunicaciones seguras en Internet o en intranets. Permitiendo a los clientes autenticar servidores y, opcionalmente, a los servidores autenticar clientes. También proporciona un canal seguro ya que cifra las comunicaciones. TLS 1.3 es la versión más reciente del protocolo Nivel de sockets seguros (SSL).

El beneficio de este cambio es que no hay necesidad de tener el servicio de acceso de clientes de RPC en el servidor acceso de clientes. Esto ocasiona la reducción de dos espacios de nombres que habitualmente se necesitarían para una solución de resistencia ante fallos a nivel de sitios.

Exchange Server 2016 incorpora protocolo de comunicación con los clientes Outlook denominado MAPI sobre HTTP (no confundir con RPC sobre HTTP o Outlook Anywhere).

MAPI sobre HTTP supone un avance importante en la simplificación de las comunicaciones de los clientes Outlook y el soporte de nuevos mecanismos de autenticación modernos como federación de identidades, autenticación de doble factor u otros.

1.1.2. EXPLOTACIÓN

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

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

1.1.2.1. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD

Se considera que IIS 10 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.

En el ENS se considera indispensable que el sistema no proporcione funcionalidades gratuitas y únicamente las estrictamente necesarias para desempeñar la función asignada. Por lo que se eliminarán o desactivarán, mediante el control de la instalación y configuración, todas aquellas funciones que no sean necesarias e incluso aquellas que sean inadecuadas al fin de preservar el principio de mínima funcionalidad establecidas en el ENS.

Para el cumplimiento del ENS, se establecen las diferentes plantillas de seguridad las cuales 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 deshabilitarán, como parte de los mecanismos de mínima funcionalidad y mínima exposición, todos aquellos procesos que pudieran implicar el envío de información al fabricante o todos aquellos servicios automatizados susceptibles de reportar datos o funcionalidad de los servidores.

1.1.2.2. OP. EXP. 4 MANTENIMIENTO

Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches y nuevas versiones publicadas por el fabricante para Exchange Server 2016.

Se tendrá en consideración las especificaciones del fabricante en lo relativo a instalación y mantenimiento de Exchange Server 2016.

Para el cumplimiento del ENS se instalarán las actualizaciones acumulativas publicadas por el fabricante de Microsoft Exchange Server 2016 las cuales solventan vulnerabilidades detectadas.

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

Exchange Server 2016 implementa mecanismos para la auditoría de los sistemas e infraestructuras. De forma predeterminada, los datos son almacenados localmente.

En las categorías media y alta del marco operacional del ENS, se deberán implementar mecanismos que garanticen la trazabilidad de las acciones de los usuarios.

En Exchange Server 2016 se registrará la actividad de los usuarios para indicar quien realiza la actividad, cuando la realiza y sobre qué información para poder detectar y reaccionar a cualquier fallo accidental o deliberado. También se contempla el registro de la actividad de los usuarios y en especial de los operadores y administradores en cuanto al acceso a la configuración y mantenimiento del Exchange Server 2016.

Deben registrarse las actividades realizadas con éxito y los intentos de fracaso.

Por lo tanto, se establece que para la categoría básica de seguridad se activaran los registros de actividad en los servidores, para la categoría media se revisaran informalmente los registros de actividad buscando patrones anormales y para la categoría alta se dispondrá de un sistema automático de recolección de registros y correlación de datos, es decir, una consola de seguridad centralizada.

1.1.2.4. OP. EXP. 9. REGISTRO DE LA GESTION DE INCIDENTES

Únicamente para las categorías media y alta de seguridad se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de tal forma que, se registrara el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

Se registrarán todas aquellas evidencias que posteriormente puedan sustentar una demanda judicial o hacer frente a ella, o cuando el incidente en cuestión pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos.

En Exchange Server 2016 existe la posibilidad de retener por juicio un buzón lo que permitirá auditar un buzón de forma transparente para el usuario previniendo con ello posibles pérdidas de información ya sean accidentales o forzosas.

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

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

a) Determinar el período de retención de los registros.

b) Asegurar fecha y hora del registro de la actividad

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

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

En Exchange Server 2016 existen grupos de roles predeterminados orientados a la protección de la información de los registros de actividad por lo que únicamente los usuarios establecidos por la organización tendrán acceso a la información de los registros de actividad.

1.2. MEDIDAS DE PROTECCIÓN

1.2.1. PROTECCIÓN DE LAS COMUNICACIONES

Para alcanzar un nivel de seguridad en las comunicaciones adecuado en el entorno o aplicación Web es necesario involucrar tanto a administradores como a desarrolladores. No es posible proporcionar un entorno Web seguro sin la colaboración de ambos grupos.

La formación de seguridad debe centrarse en proporcionar un conocimiento adecuado a administradores y desarrolladores respecto a las vulnerabilidades y amenazas de seguridad en entornos Web, los diferentes tipos de ataques existentes y los mecanismos de defensa asociados, preferiblemente mediante ejemplos prácticos.

El Real Decreto 3/2010 de 8 de enero, de desarrollo del Esquema Nacional de Seguridad 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 por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

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 detectados, permitiendo activarse los procedimientos previstos en el tratamiento frente a incidentes usando los mecanismos de autenticación establecidos anteriormente expuestos en este documento en el punto "1.1.1.4 OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN".

En aquellos sistemas en que sea de aplicación la categoría media de seguridad del ENS, 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 categoría alta de seguridad del ENS, es recomendable el empleo de dispositivos de hardware para el establecimiento de la comunicación y la utilización de redes virtuales privadas, frente a soluciones de tipo software. Se deberán tener en consideración únicamente los productos que se encuentran certificados y acreditados para tal efecto.

Se establecerá una prevención activa de ataques garantizando, como mínimo, que estos sean detectados, y se procederá a activar los procedimientos previstos en el tratamiento de incidentes de los cuales se consideran ataques activos los siguientes supuestos:

a) La alteración de la información en el tránsito de la comunicación.

b) La inyección de información ilegitima en la comunicación con un fin fraudulento.

c) El secuestro de una sesión por una tercera parte.

Se deberán aplicar los últimos parches de seguridad en cada uno de los elementos software que forman parte de la plataforma de Exchange Server 2016: software de los dispositivos de red y firewalls, sistema operativo de los servidores (Web, aplicación, y base de datos).

1.2.1.2. MP. COM. 9. MEDIOS ALTERNATIVOS

En la categoría alta de seguridad del ENS se establece que se deberá garantizar la existencia y disponibilidad de medios alternativos en caso de que fallen los medios habituales por ello Exchange Server 2016 utiliza, tanto para la alta disponibilidad como para la resistencia de sitio, un concepto conocido como implementación incremental. Para ello se debe disponer de dos o más servidores de buzones de correo de Exchange 2016 como servidores independientes y, luego, configurarlos de manera incremental junto con las bases de datos de buzones de correo para que haya una alta disponibilidad y resistencia de sitios según sea necesario.

Microsoft Exchange Server 2016, implementa la alta disponibilidad del transporte de la información la cual es responsable de mantener copias redundantes de los mensajes antes y después de la entrega correcta de estos.

1.2.1.3. MP. SI. 5. BORRADO Y DESTRUCCION

Las medidas de borrado y destrucción de información se aplicarán a todo tipo de equipos susceptibles de almacenar información.

Microsoft Exchange Server 2016 permite eliminar una base de datos de buzones o un buzón de una base de datos, pero se debe tener en cuenta que el usuario que realiza la acción debe tener los permisos adecuados y una vez desvinculado se deberá eliminar físicamente la carpeta contenedora de la información, y si desea eliminar el soporte de dicha información deberá proceder siguiendo el procedimiento marcado en el borrado y destrucción de soportes físicos que establece el ENS.

Nota: Si desea obtener más información sobre el borrado de bases de datos de buzones de correo puede visitar el sitio web: https://technet.microsoft.com/es-es/library/bb201683(v=exchg.141).aspx.

1.2.1.4. MP. INFO. 3. CIFRADO DE LA INFORMACIÓN

El ENS establece que las organizaciones cuya información este categorizada como categoría alta debe estar cifrada para evitar con ello que sea sustraída en caso de intercepción de la información emitida en un correo electrónico.

Cada organización debe analizar la conveniencia de implantar controles y herramientas para el cifrado y firma del correo electrónico de acreditada robustez, que empleen algoritmos acreditados por el Centro Criptológico Nacional y preferentemente productos certificados en el caso de entornos de categoría alta.

Exchange Server 2016 permite implementar mecanismos de cifrado y control de la información adicionales como S/MIME y derechos de información (IRM). Exchange Server 2016 proporciona agentes IRM que permiten aplicar plantillas de seguridad en los mensajes en tránsito de forma automática, antes de salir de la organización.

S/MIME permite cifrar mensajes de correo electrónico y firmarlos digitalmente. Cuando se usa S/MIME con un mensaje de correo electrónico, los destinatarios pueden comprobar que lo que ven en sus bandejas de entrada es el mensaje exacto que envió el remitente, además, proporciona servicios de seguridad criptográfica como autenticación, integridad de mensajes y no rechazo de origen (usando firmas digitales).

1.2.1.5. MP. INFO. 4. FIRMA ELECTRONICA

Exchange Server 2016 permite firmar digitalmente un mensaje de correo, el cual aplica una marca digital única al mensaje. La firma digital incluye el certificado y la clave pública, que proceden del Id. digital. Un mensaje firmado digitalmente garantiza al destinatario que el usuario, y no un impostor, ha firmado el contenido del mensaje y que el contenido no se ha modificado durante la transmisión.

Las firmas digitales son el servicio más utilizado de S/MIME. Como su nombre indica, las firmas digitales son la contrapartida digital a la tradicional firma legal en un documento impreso. Al igual que ocurre con una firma legal, las firmas digitales ofrecen las diferentes capacidades de seguridad:

a) Autenticación. Una firma sirve para validar una identidad. Comprueba la respuesta a "quién es usted" al ofrecer una forma de diferenciar esa entidad de todas las demás y demostrar su unicidad. Como no existe autenticación en el correo electrónico SMTP, no hay ninguna forma de saber quién envió realmente un mensaje. La autenticación en una firma digital resuelve este problema al permitir que un destinatario sepa que un mensaje fue enviado por la persona o la organización que dice haber enviado el mensaje.

b) No rechazo. La unicidad de una firma impide que el propietario de la firma no reconozca su firma. Esta capacidad se llama no rechazo. Así, la autenticación proporcionada por una firma aporta el medio de exigir el no rechazo. El concepto de no rechazo resulta más familiar en el contexto de los contratos en papel: un contrato firmado es un documento legalmente vinculante y es imposible no reconocer una firma autenticada. Las firmas digitales ofrecen la misma función y, cada vez en más áreas, se reconocen como legalmente vinculantes, de manera similar a una firma en un papel. Como el correo electrónico SMTP no ofrece ningún medio de autenticación, no puede proporcionar la función de no rechazo. Para el remitente de un mensaje de correo electrónico SMTP es fácil no reconocer la propiedad del mismo.

c) Integridad de los datos. Un servicio de seguridad adicional que ofrecen las firmas digitales es la integridad de los datos. La integridad de los datos es uno de los resultados de las operaciones que hacen posibles las firmas digitales. Con los servicios de integridad de datos, cuando el destinatario de un mensaje de correo electrónico firmado digitalmente valida la firma digital, tiene la seguridad de que el mensaje recibido es el mismo mensaje que se firmó y se envió, y que no se ha manipulado mientras estaba en tránsito. Cualquier alteración del mensaje mientras estaba en tránsito una vez firmado invalida la firma. De esta forma, las firmas digitales son capaces de ofrecer una garantía que no permiten tener las firmas en papel, ya que es posible alterar un documento en papel una vez que ha sido firmado.

1.2.1.6. MP. INFO. 9. COPIAS DE SEGURIDAD (BACKUP)

Exchange Server 2016 usa un concepto conocido como Exchange Native Data Protection, el cual se basa en características integradas de Exchange para proteger los datos de su buzón de correo sin tener que usar copias de seguridad.

Exchange Server 2016 incluye varias características que, una vez implementados y configurados correctamente, ofrecen una protección de datos nativa que puede llegar a eliminar la necesidad de realizar copias de datos tradicionales.

Exchange Server 2016 incluye un complemento para Copias de seguridad de Windows Server que permite realizar y restaurar copias de seguridad basadas en VSS de datos de Exchange.

1.2.1.7. MP. S. 1. PROTECCIÓN DEL CORREO ELECTRONICO

En Microsoft Exchange Server 2016, Information Rights Management (IRM) está habilitado por defecto para los mensajes internos. Esto permite crear reglas de protección de transporte y reglas de protección de Microsoft Outlook para proteger con IRM los mensajes durante el transporte y en los clientes de Microsoft Outlook 2010 y posteriores.

Habilitar IRM para los mensajes internos es un requisito previo para el resto de funciones de IRM de Exchange Server 2016 como el descifrado de transporte, el descifrado de reglas del diario, IRM en Microsoft Office Outlook Web App e IRM en Microsoft Exchange ActiveSync.

En Exchange Server 2016, las reglas de protección de Outlook ayudan a la organización a protegerse ante el riesgo de filtraciones de información mediante la aplicación automática de la protección de IRM a los mensajes de Exchange 2016. Los mensajes se protegen con IRM antes de abandonar al cliente de Outlook, incluyendo los datos adjuntos que usan formatos de archivo compatibles.

1.2.1.8. MP. S. 2. PROTECCIÓN DE SERVICIOS Y APLICACIONES WEB

Exchange Server 2016 utiliza IIS por lo que todos los sistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que le competen como:

a) Ataques directos, tales como accesos no autorizados sobre cualquiera de los elementos que conforman el entorno o aplicación Web.

b) Ataques indirectos, dónde cualquiera de los elementos es empleado como herramienta en el ataque. Por ejemplo, un ataque sobre los servidores de DNS podría permitir redireccionar el tráfico de los clientes Web hacia un entorno malicioso que suplante la aplicación Web real.

c) Ataques de denegación de servicio (DoS). Las arquitecturas Web están basadas en tecnologías TCP/IP y por tanto son vulnerables a los ataques de DoS comunes en TCP/IP. Es necesario disponer de contramedidas técnicas y procedimientos de actuación frente a este tipo de ataques.

Se deberán aplicar los últimos parches de seguridad en cada uno de los elementos software que forman parte de la plataforma de la aplicación Web: software de los dispositivos de red y firewalls, sistema operativo de los servidores (Web, aplicación, y base de datos), y software de la plataforma de desarrollo empleada (PHP, ASP, Java, etc.).

1.2.1.9. MP. S. 9. MEDIOS ALTERNATIVOS

En la categoría alta de seguridad del ENS se establece que se deberá garantizar la existencia y disponibilidad de medios alternativos en caso de que fallen los medios habituales por ello Exchange Server 2016 utiliza, tanto para la alta disponibilidad como para la resistencia de sitio, un concepto conocido como implementación incremental. Para ello se debe disponer de dos o más servidores de buzones de correo de Exchange 2016 como servidores independientes y, luego, configurarlos de manera incremental junto con las bases de datos de buzones de correo para que haya una alta disponibilidad y resistencia de sitios según sea necesario.

Microsoft Exchange Server 2016, implementa la alta disponibilidad del transporte de la información la cual es responsable de mantener copias redundantes de los mensajes antes y después de la entrega correcta de estos.

2. RESUMEN Y APLICACIÓN DE MEDIDAS DE EXCHANGE SERVER 2016 SOBRE MS WINDOWS SERVER 2016

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

Control	Medida	Mecanismo de aplicación
OP. ACC. 1	Segregación de roles y tareas	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
OP. ACC. 3	Gestión de derechos de acceso	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.

Control	Medida	Mecanismo de aplicación
OP. ACC. 4	Proceso de gestión de derechos de acceso	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
OP. ACC. 5	Mecanismos de autenticación	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
OP. ACC. 7	Protocolos de autenticación en red	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
OP. EXP. 2	Control de funcionalidad de servicios para garantizar el principio de mínima funcionalidad	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
OP. EXP. 4	Gestión de la configuración	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
OP. EXP. 8	Registro de actividad de los usuarios	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización. Se debe tomar en consideración que el RD 951/2015 cambia la medida con respecto a lo establecido en RD 3/2010. En la actualidad el requisito del registro de actividad es requerido desde la categoría básica. Revisión e implementación guía CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2.
OP. EXP. 9	Registro de la gestión de incidentes	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
OP. EXP. 10	Protección de los registros de actividad	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
MP. COM. 3	Protección de la autenticación y de la integridad	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
MP. COM. 9	Medios alternativos	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
MP. SI. 5	Borrado y destrucción de la información	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
MP. INFO. 3	Cifrado de la información	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
MP. INFO. 4	Firma electrónica de la información	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
MP. INFO. 9	Copia de seguridad	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
MP. S. 1	Protección del correo electrónico	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
MP. S. 2	Protección de servicios y aplicaciones web	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.
MP. S. 9	Medios alternativos	Revisión e implementación de guía CCN-STIC-576, adaptándolos a la organización.

ANEXO A.2. CATEGORÍA BÁSICA

ANEXO A.2.1. PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE EXCHANGE SERVER 2016 SOBRE MICROSOFT 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 emplee el producto Microsoft Exchange Server 2016 sobre Windows 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 la categoría de cada una de las dimensiones de seguridad, según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran 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, se deberán realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

Microsoft Exchange Server 2016 requiere de otros servicios adicionales para su instalación y correcto funcionamiento, por lo que es necesario realizar una preparación previa del entorno antes de instalar Microsoft Exchange Server 2016.

En caso de necesitar información sobre los requisitos previos de instalación de Microsoft Exchange Server 2016, visite el siguiente enlace: https://docs.microsoft.com/es-es/Exchange/plan-and-deploy/prerequisites?view=exchserver -2016

Antes de iniciar las operaciones de implementación es necesario disponer de los siguientes elementos:

a) Un servidor controlador de dominio Windows Server 2016 que haya sido preparado siguiendo la guía de seguridad CCN-STIC-570A Anexo A con una categorización de seguridad básica.

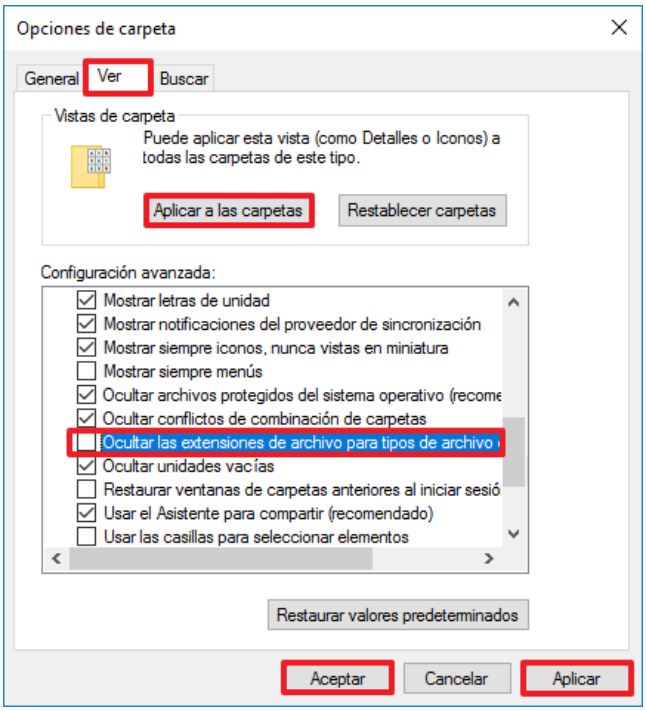
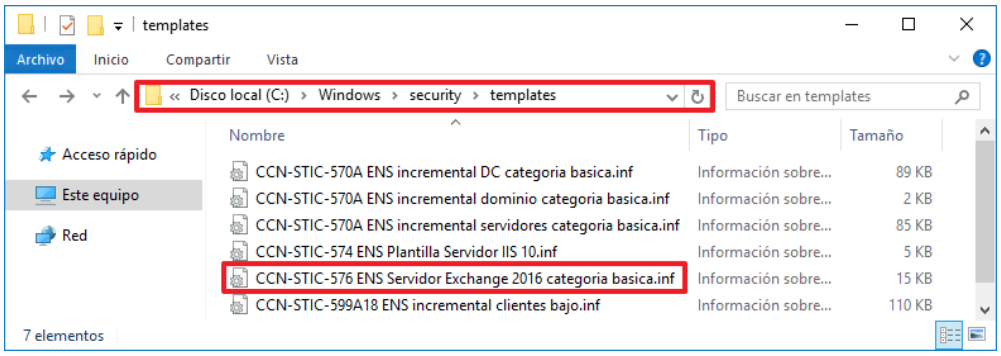
b) Un servidor miembro del dominio con el servicio Web Internet Information Services instalado y preparado siguiendo las guías CCN-STIC-570A Anexo A y CCN-STIC-574 Anexo A con una categorización de seguridad básica.

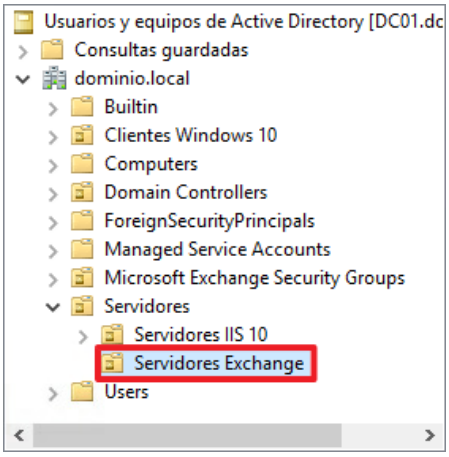
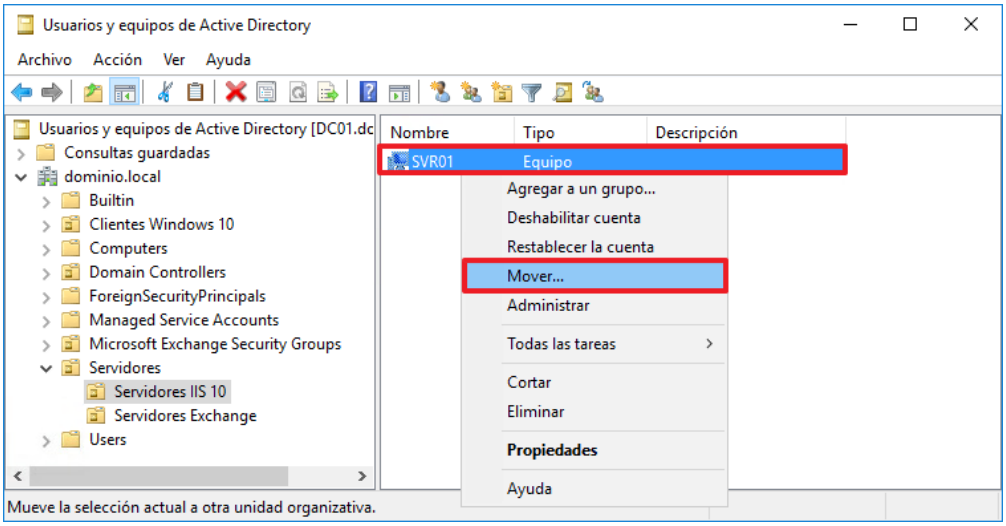
1. PREPARACIÓN DEL DOMINIO

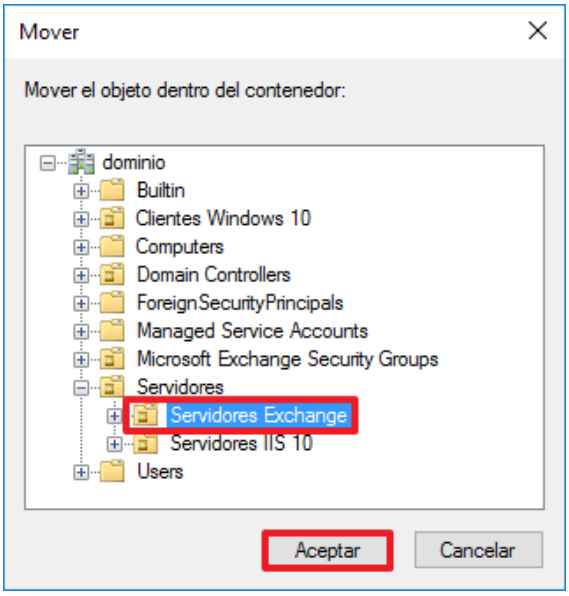
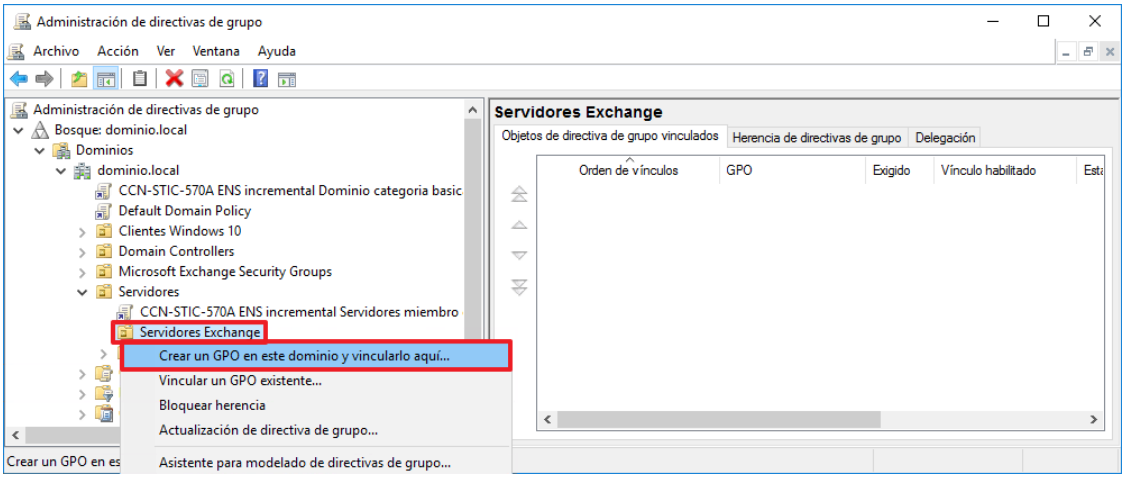
Los pasos que se describen a continuación se realizarán en un controlador del dominio al que va a pertenecer el servidor miembro que contenga Microsoft Exchange Server 2016. Estos pasos sólo se realizarán cuando se incluya el primer servidor de Microsoft Exchange Server 2016 que actúe como miembro del dominio. Durante este procedimiento se crea la unidad organizativa que contiene los servidores de correo y se realizan las configuraciones de políticas de grupo correspondientes.

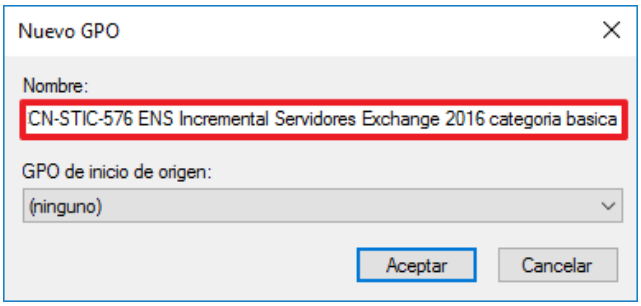
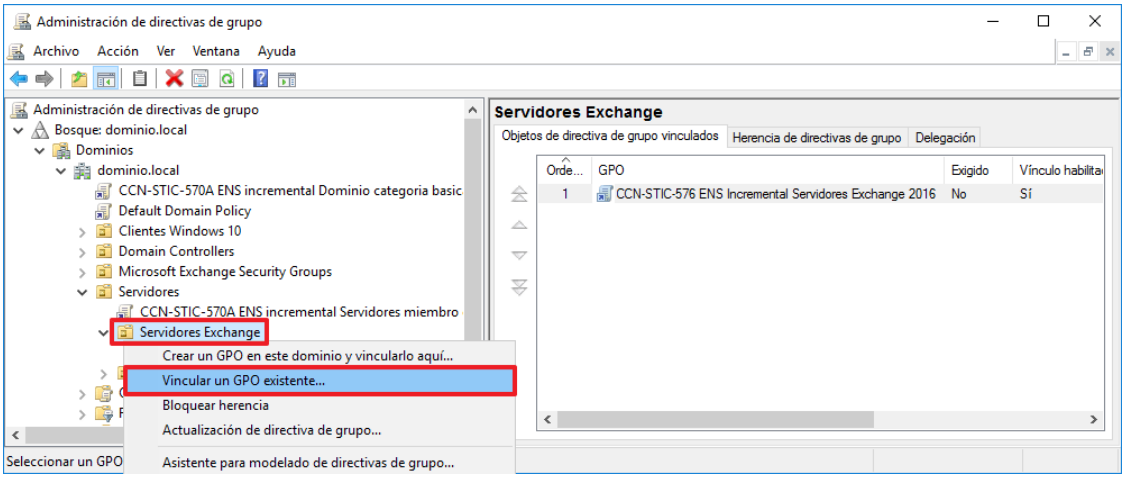
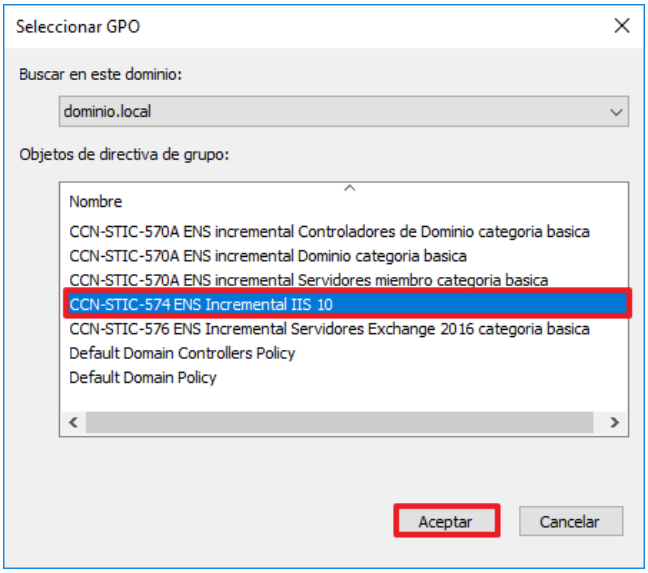
Nota: Esta guía asume que los servidores Controladores del Dominio al que pertenece el equipo servidor de Exchange que está asegurando, se les ha aplicado la configuración descrita en la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016". Si no es así, aplique la guía correspondiente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

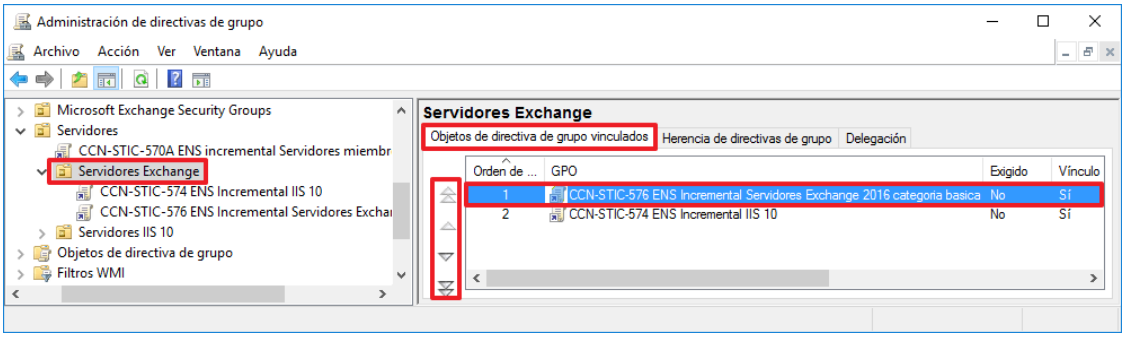
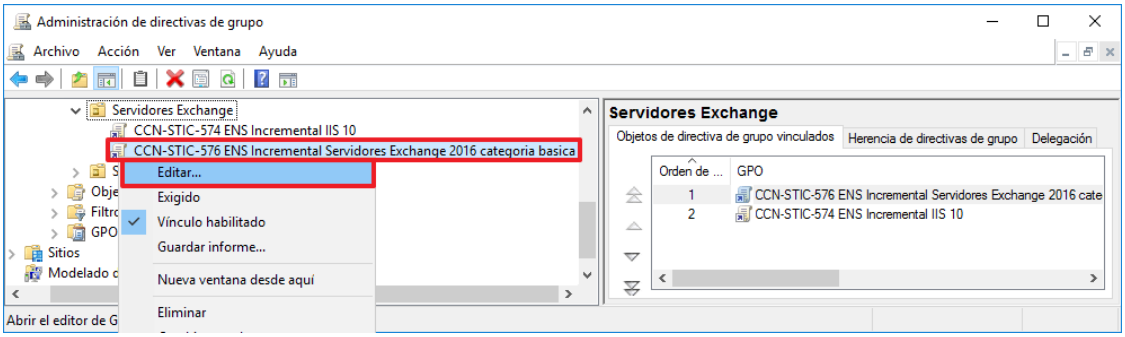
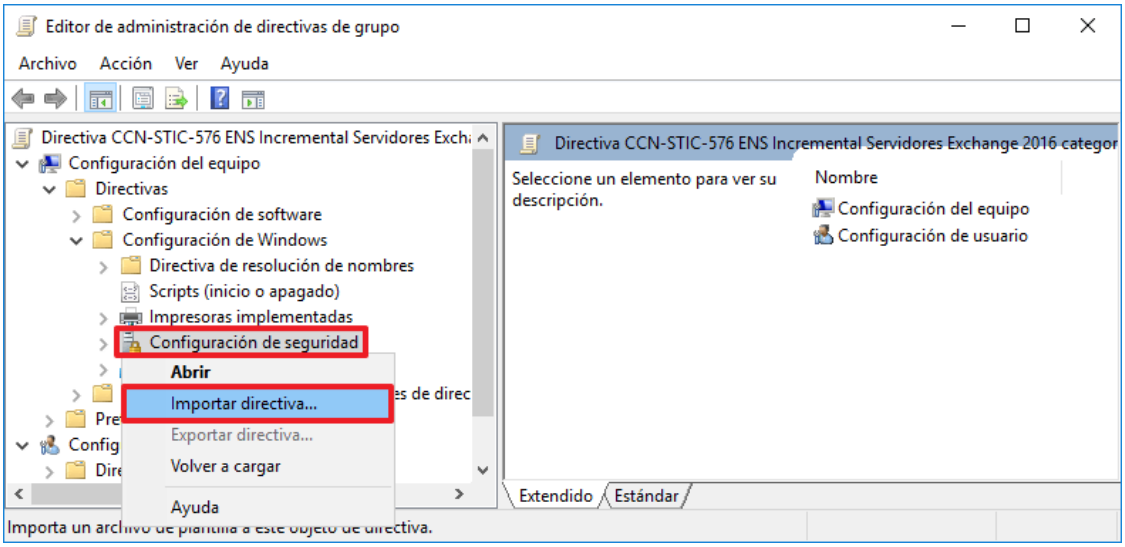
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
2.	Cree el directorio "Scripts" en la unidad "C:\". **Nota:** Los scripts asumen que su ubicación en el sistema será bajo "C:\Scripts". Si los colocara en otra ubicación, tendría 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.	Configure el "Explorador de Windows" para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que "Explorador de Windows" muestra las extensiones de los archivos.

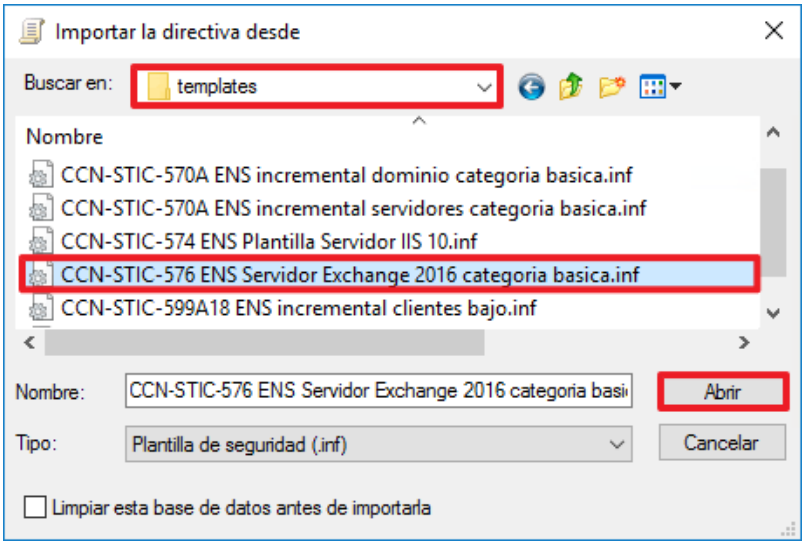
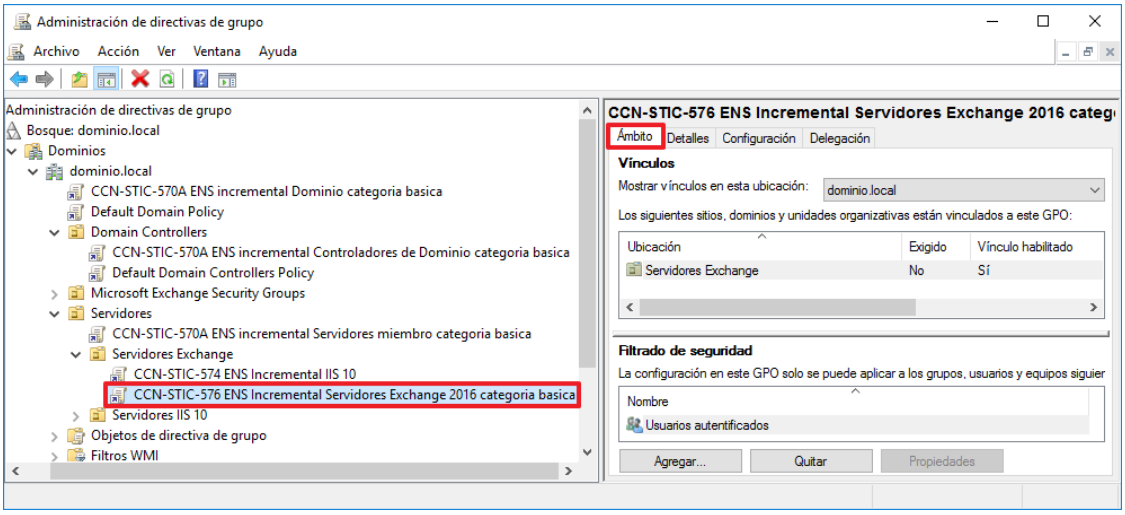
Paso	Descripción
5.	Para configurar el "Explorador de Windows" de modo que muestre las extensiones de todos los archivos, abra una ventana de "Explorador de Windows", seleccione en el menú superior, "Vista" y dentro de dicho menú, "Opciones" de la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".
6.	Copie los ficheros "CCN-STIC-576 ENS Servidor Exchange 2016 categoria basica.inf" al directorio "C:\Windows\Security\Templates" del Controlador de Dominio.  **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón "Continuar" y pulse "Sí" con una cuenta la cual debe ser al menos administrador de dominio.

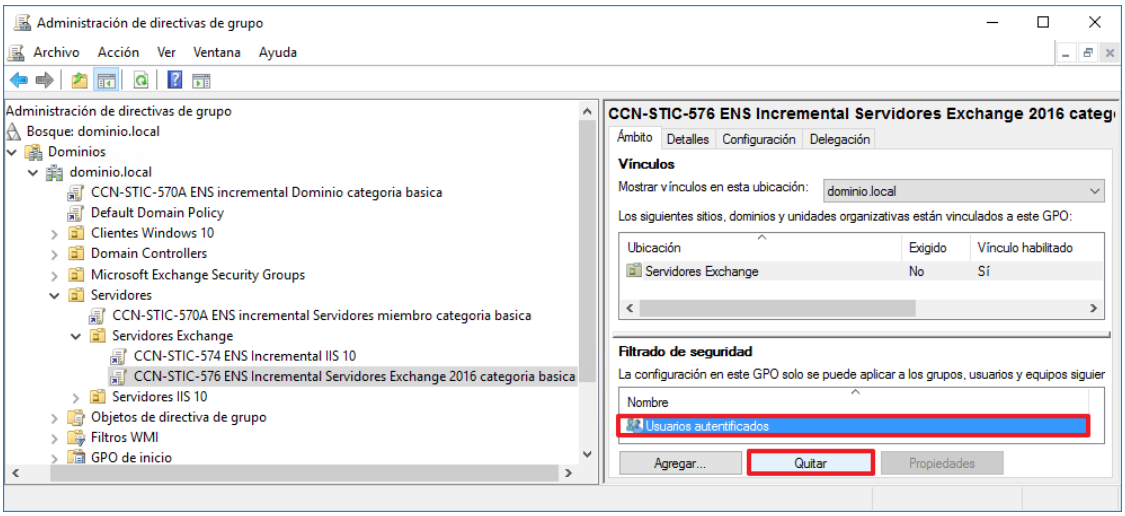
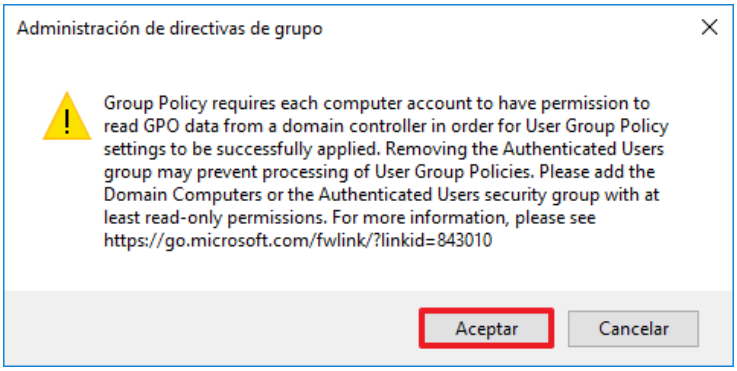
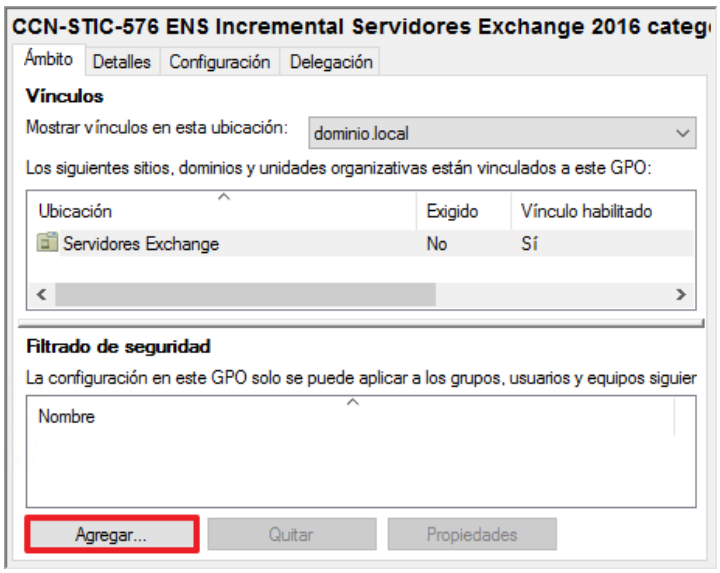
Paso	Descripción
7.	Ejecute la consola administrativa Usuarios y Equipos de Directorio Activo desde el Administrador del servidor **"Herramientas → Usuarios y Equipos de Active Directory"**. **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el menú de inicio. Si lo inicia por primera vez, el control de cuentas de usuario le solicitará permiso para iniciar el Administrador del servidor.
8.	En la consola, cree una nueva unidad organizativa denominada "Servidores Exchange" dependiendo de la unidad organizativa "Servidores", tal y como se muestra en la imagen.  **Nota:** En este ejemplo se crea la nueva unidad organizativa bajo "Servidores". Modifique este paso de acuerdo con las necesidades del entorno de su organización.
9.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores que contengan Exchange Server 2016 a la unidad organizativa "Servidores Exchange". Para ello, deberá hacer clic botón derecho sobre "Mover" en el servidor que desee ubicar en la nueva unidad organizativa.  **Nota:** Si ha seguido los pasos de la guía "CCN-STIC-574 Implementación del ENS en IIS 10 sobre Windows Server 2016" el servidor se encontrará bajo la unidad organizativa "Servidores IIS 10".

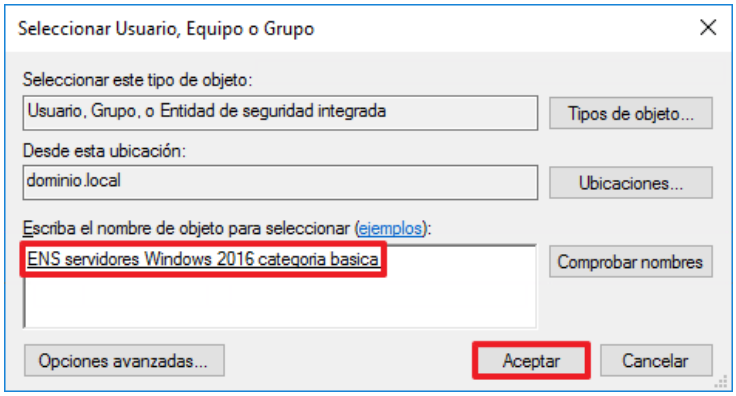
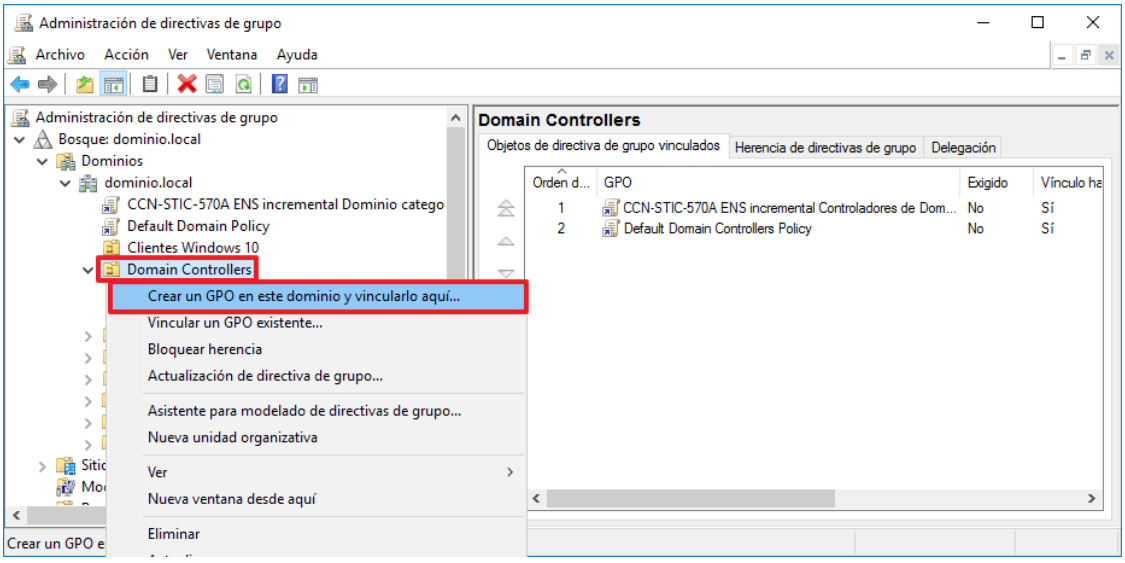
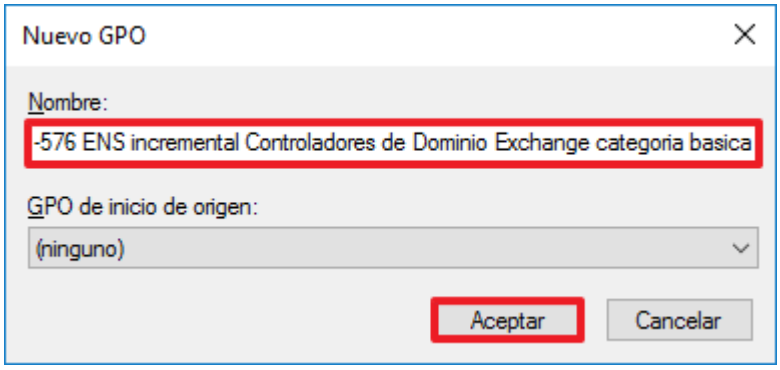
Paso	Descripción
10.	A continuación, seleccione la unidad organizativa "Servidores Exchange". 
11.	Cierre la herramienta de "Usuarios y equipos de Directorio Activo"
12.	Una vez realizada la preparación del Directorio Activo que dará servicio a Exchange Server 2016, deberá realizar el resto de preparación y configuración de políticas de seguridad. Para ello, inicie la consola de administración de directivas de grupo desde el Administrador del servidor en el menú **"Herramientas → Administración de directivas de grupo"**.
13.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa recién creada "Servidores Exchange", haciendo clic con el botón derecho en el menú "Crear un GPO en este dominio y vincularlo aquí…". 

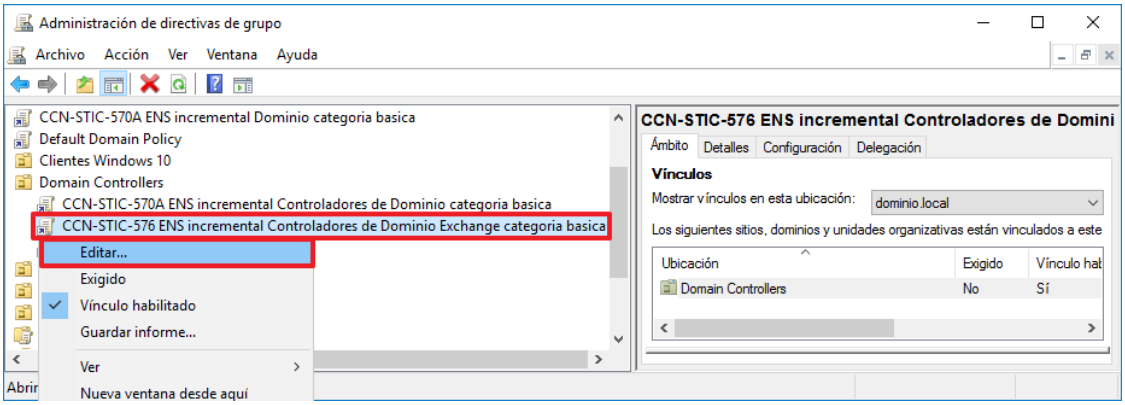
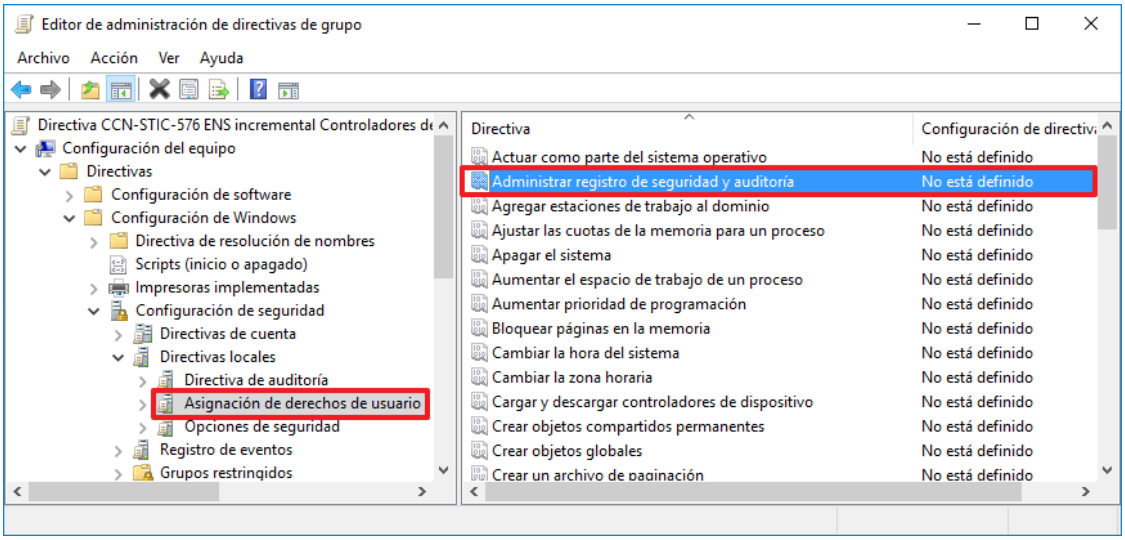
Paso	Descripción
14.	Escriba el nombre de la GPO "CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria basica" y haga clic en el botón "Aceptar". 
15.	A continuación, se va a vincular la GPO "CCN-STIC-574 ENS Incremental IIS 10" de la guía "CCN-STIC-574 Implementación del ENS en IIS 10 sobre Windows Server 2016", en la unidad organizativa "Servidores Exchange" creada en pasos anteriores.
16.	Pulse botón derecho sobre la unidad organizativa "Servidores Exchange" y haga clic sobre "Vincular un GPO existente…". 
17.	A continuación, seleccione el objeto de directiva de grupo: "CCN-STIC-574 ENS Incremental IIS 10" y pulse sobre aceptar. 

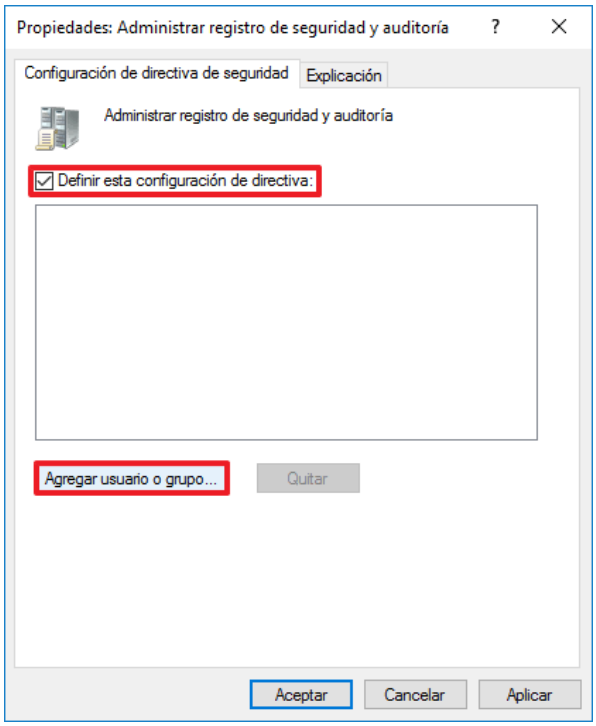
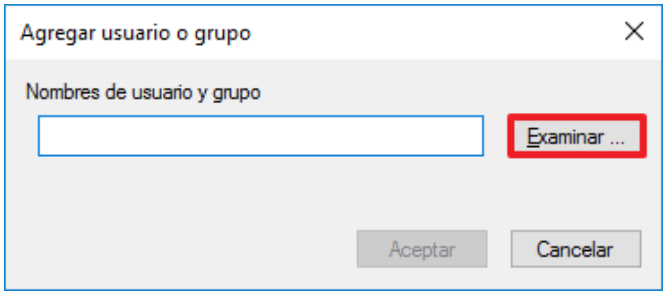
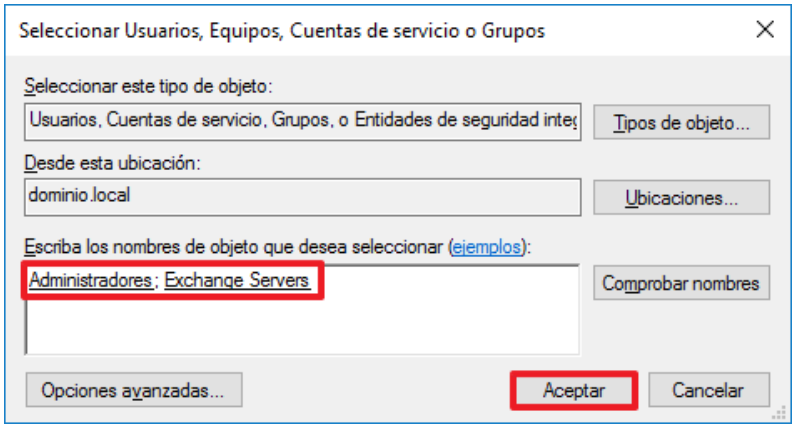
Paso	Descripción
18.	Para que la aplicación de las directivas se realice en el orden correcto, asegúrese de que la directiva "CCN-STIC-576 ENS Incremental Servidor Exchange 2016 categoria basica" aparezca en primer lugar. Para ello seleccione, dentro de la unidad organizativa, la directiva "CCN-STIC-576 ENS Incremental Servidor Exchange 2016 categoria basica" y a continuación, haga clic sobre la flecha doble hacia arriba para que se sitúe en primer lugar del orden vínculos, tal y como se muestra en la imagen. 
19.	A continuación, edite la GPO: "CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria basica" creada anteriormente haciendo clic con el botón derecho en ella y seleccionando el menú "Editar". 
20.	Expanda el nodo **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad"**.
21.	A continuación, haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva...". 

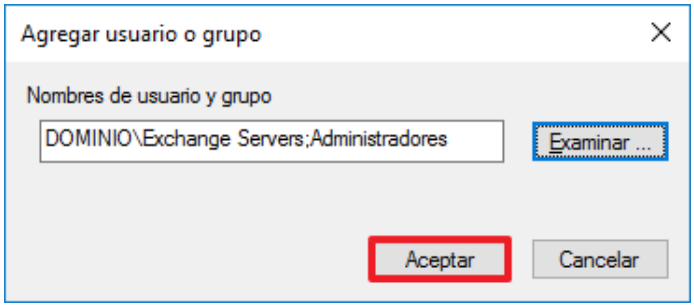
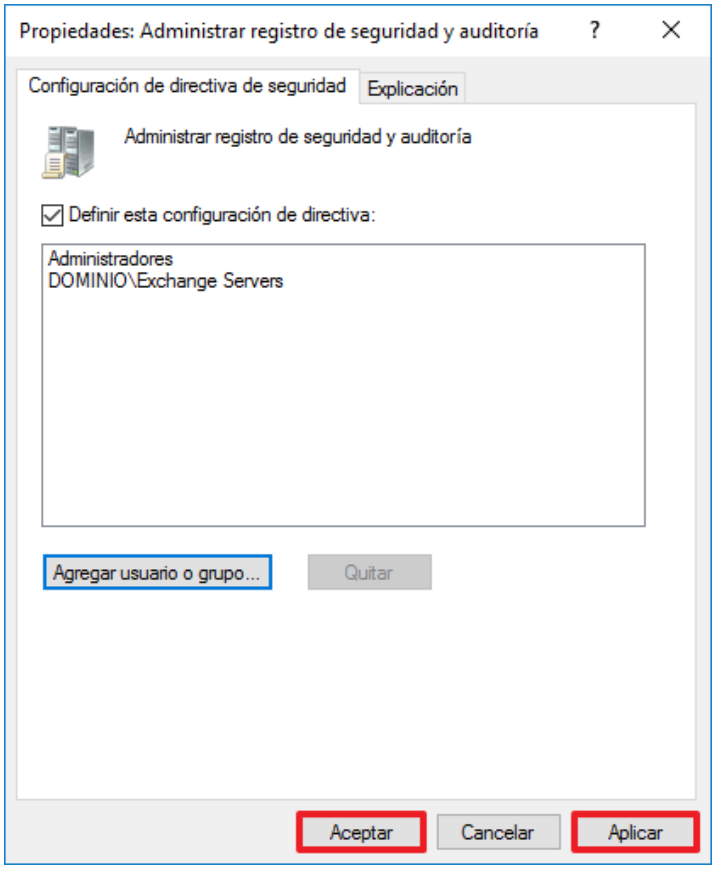
Paso	Descripción
22.	Importe la plantilla de seguridad "CCN-STIC-576 ENS Servidor Exchange 2016 categoria basica.inf" que previamente debe haberse copiado en la ruta "C:\Windows\Security\Templates" y haga clic en botón "Abrir". 
23.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
24.	Seleccione la nueva política de grupo configurada y vaya a la pestaña "Ámbito" que se encuentra en el panel derecho. 

Paso	Descripción
25.	En la opción de filtrado de seguridad, seleccione "Usuarios autentificados" y pulse la opción "Quitar". 
26.	Pulse el botón "Aceptar" cuando le pregunte si desea quitar este privilegio de delegación.
27.	Pulse "Aceptar" sobre la advertencia que se mostrará en una ventana emergente. 
28.	Una vez quitado, pulse el botón "Agregar...". 

Paso	Descripción
29.	Introduzca como nombre "ENS servidores Windows 2016 categoria basica". Este grupo corresponde con el generado en la aplicación de la guía codificada como "CCN-STIC-570A". A continuación, pulse el botón "Aceptar".  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.
30.	Pulse con botón derecho sobre la unidad organizativa "Domain Controllers" y seleccione "Crear un GPO en este dominio y vincularlo aquí…". 
31.	Introduzca el nombre "CCN-STIC-576 incremental Controladores de Dominio Exchange categoria basica" y pulse "Aceptar". 

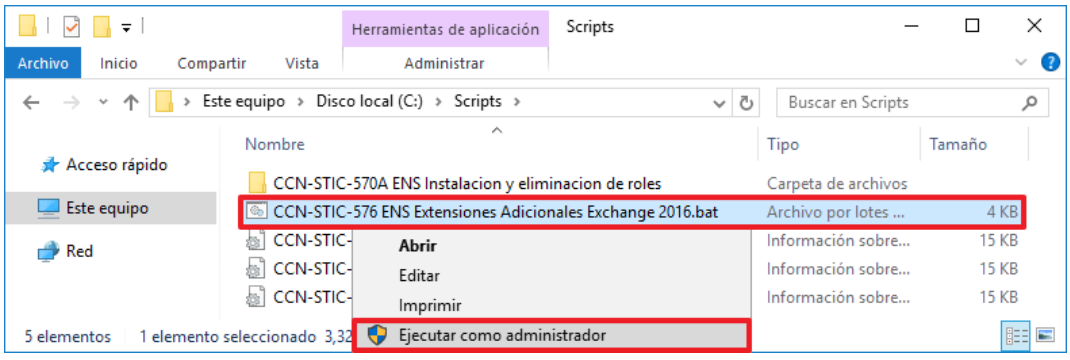
Paso	Descripción
32.	Seleccione la GPO recién creada y pulse "Editar…". 
33.	Despliegue el nodo **"Directiva CCN-STIC-576 incremental Controladores de Dominio Exchange categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"** y haga doble clic sobre la directiva "Administrar registro de seguridad y auditoría". 

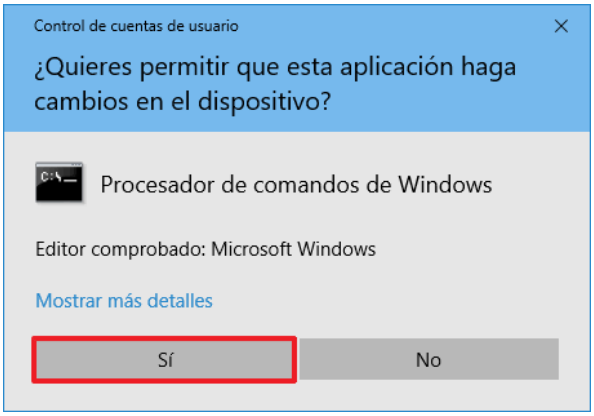
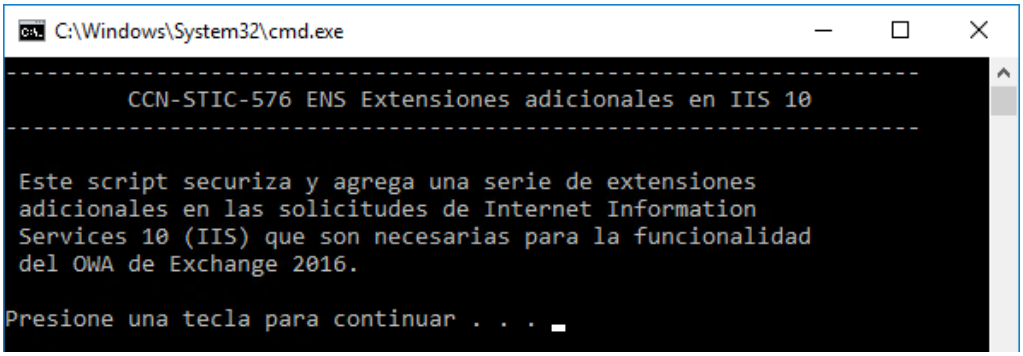
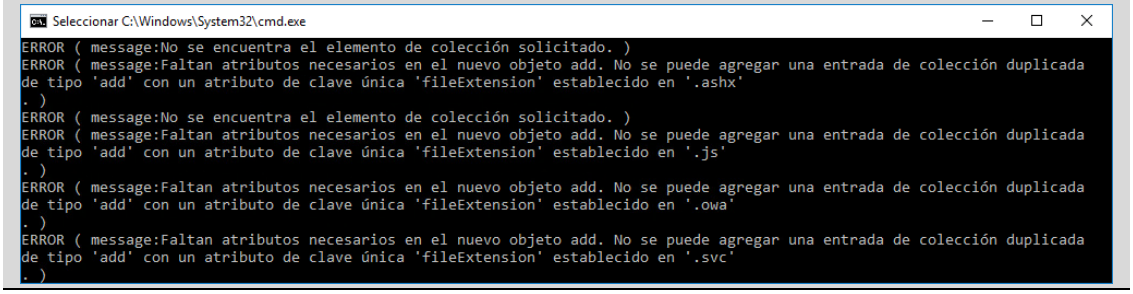
Paso	Descripción
34.	Marque la casilla "Definir esta configuración de directiva:" y pulse sobre "Agregar usuario o grupo…". 
35.	Pulse sobre "Examinar". 
36.	Añada los grupos "Administradores" y "Exchange Servers". Pulse "Aceptar". 

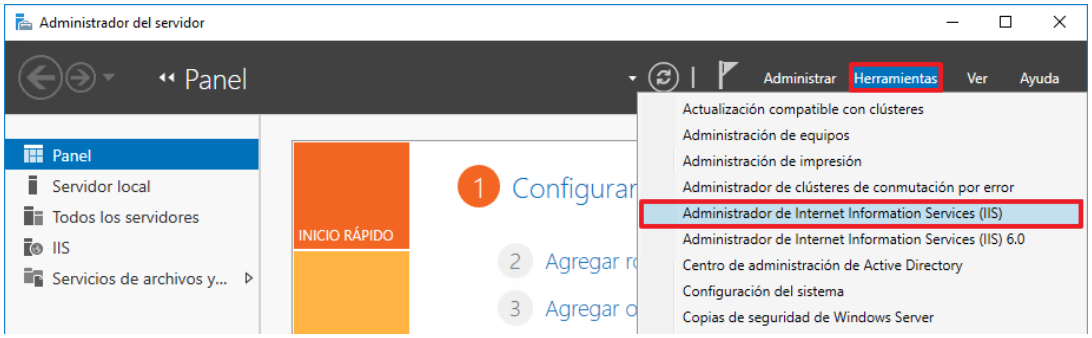
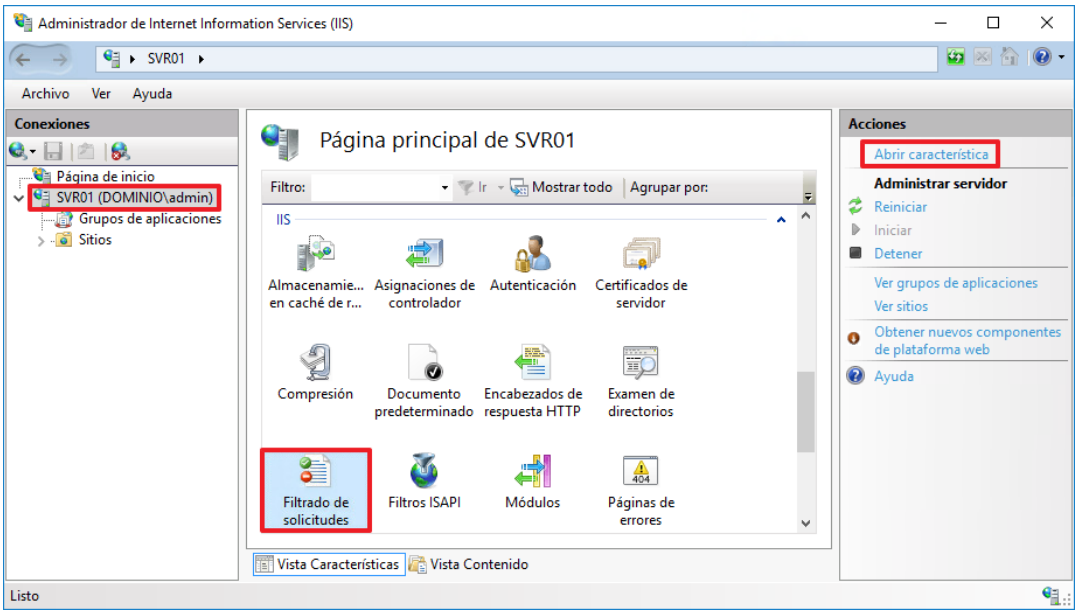
Paso	Descripción
37.	Pulse nuevamente sobre "Aceptar". 
38.	Para finalizar pulse sobre "Aplicar" y "Aceptar". 
39.	Cierre todas las ventanas de administración y borre la carpeta "C:\Scripts".
40.	Reinicie los servidores para que se hagan efectivos los cambios.

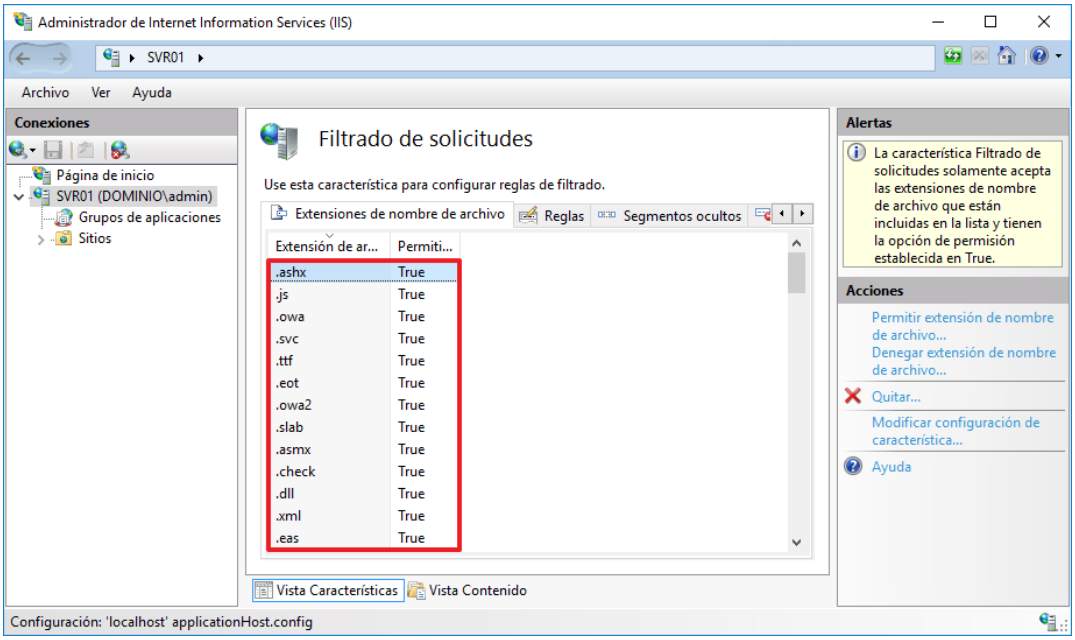
2. PREPARACIÓN DEL IIS 10

Los pasos que se describen a continuación se realizarán en un servidor miembro del dominio al que pertenece el servidor Exchange Server 2016.

Paso	Descripción
41.	Inicie sesión en el servidor miembro donde tenga instalado IIS 10 para agregar las extensiones necesarias para el funcionamiento correcto de Exchange Server 2016.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
42.	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, tendría que editar los scripts para reflejar la nueva ubicación.
43.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".
44.	Ejecutar el script que permite agregar extensiones al servidor IIS 10. Por lo tanto, con el botón derecho seleccione el fichero denominado "CCN-STIC-576 ENS Extensiones adicionales Exchange 2016.bat" y seleccione "Ejecutar como administrador". 

Paso	Descripción
45.	El control de cuentas de usuario le solicitará elevación de privilegios. 
46.	Aparecerá la siguiente pantalla. Pulse una tecla para continuar.  **Nota:** Si tras la ejecución del script aparece un mensaje de error advirtiendo de que no se puede agregar una entrada de colección duplicada, significa que este procedimiento se ha realizado anteriormente. Omita dicho error y continúe con la ejecución del siguiente paso. 
47.	Cuando haya finalizado la ejecución, pulse una tecla para cerrar la ventana.

Paso	Descripción
48.	Compruebe que se ha aplicado correctamente la configuración de las extensiones, para ello, diríjase al administrador de IIS dentro del desplegable "Herramientas" del "Administrador del servidor". 
49.	Compruebe que se ha aplicado correctamente la configuración de las extensiones, para ello, diríjase al administrador de IIS, seleccione la opción "Filtrado de solicitudes" y en el menú situado en el lateral derecho, pulse "Abrir característica". 

Paso	Descripción
50.	Compruebe que las extensiones de nombre de archivo específicas para Exchange Server 2016 están configuradas correctamente en la columna "Permitido" en "True". Para ello diríjase a la pestaña "Extensiones de nombre de archivo". – .ashx – .js – .owa – .svc – .ttf – .eot – .owa2 – .slab – .asmx – .check – .dll – .eas  **Nota:** En caso de que no aparezca reflejada alguna de las extensiones de nombre de archivo arriba referenciadas, deberá crearlas a mano a través del menú "Acciones" situado a la derecha.
51.	Una vez realizada la comprobación cierre el administrador de Internet Information Services.

3. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

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

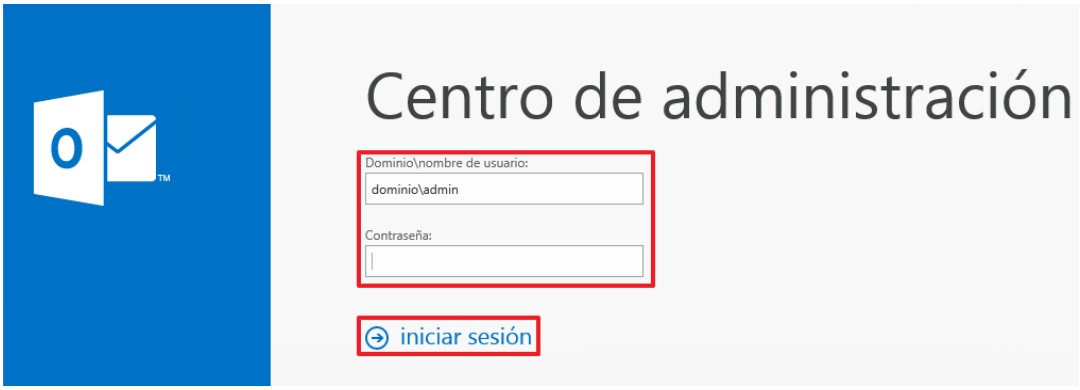
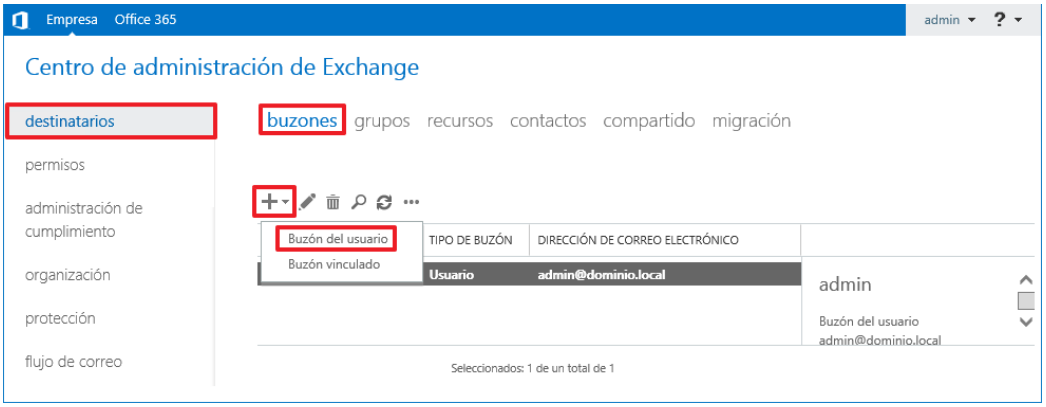
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

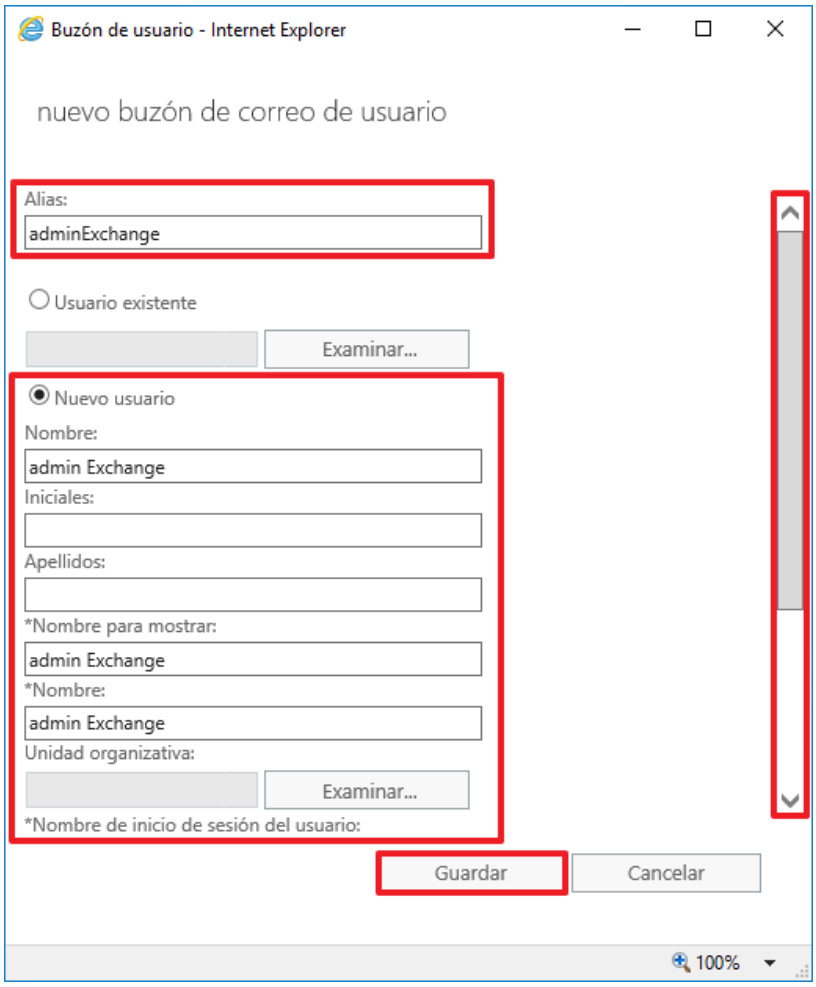
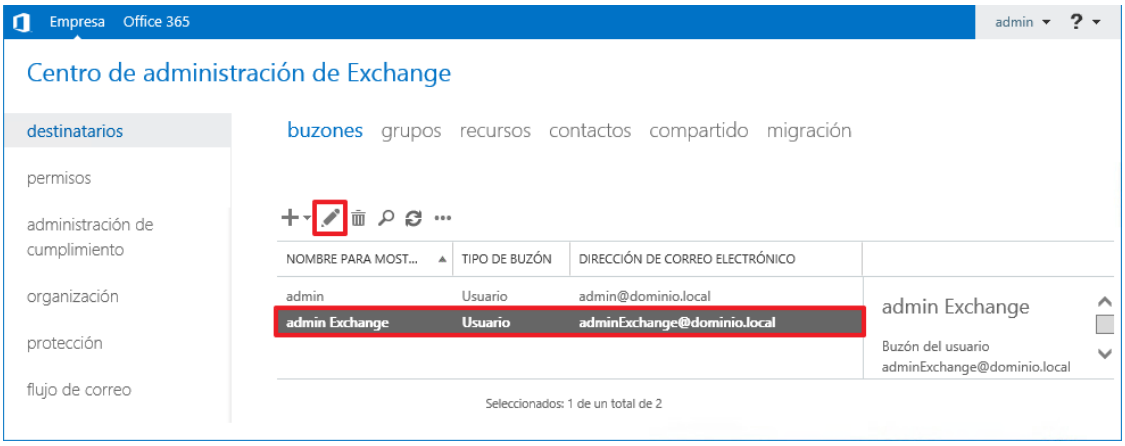
Nota: Todas las recomendaciones de seguridad indicadas en la presente guía deben ser adaptadas al entorno de su organización. Se aconseja realizar las pruebas pertinentes en un entorno de preproducción antes de ser incluidas en su entorno de producción.

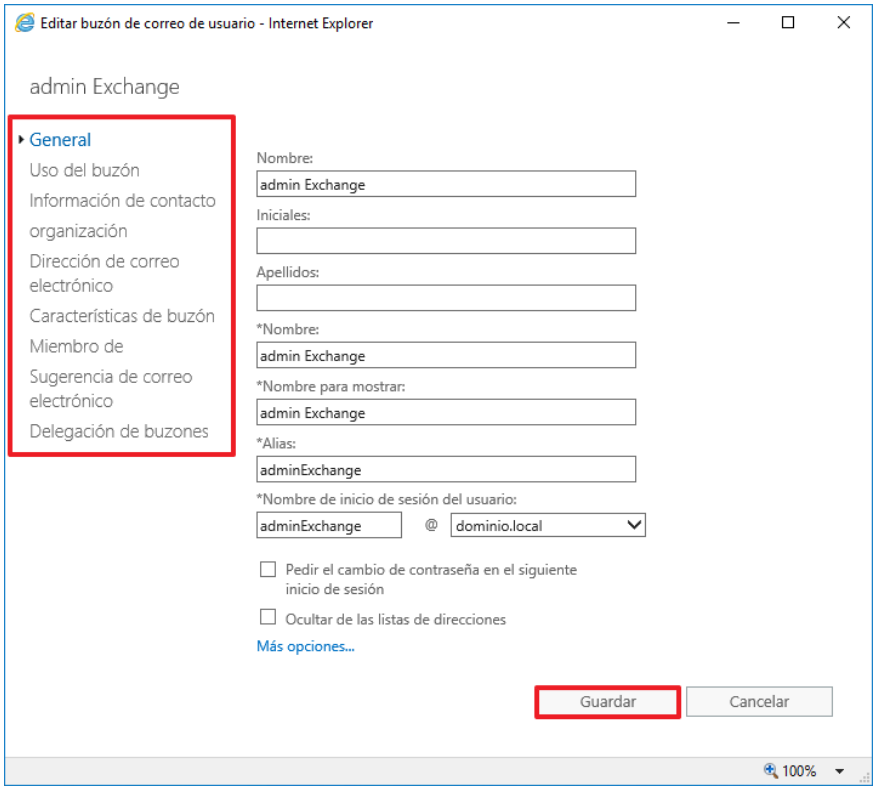
3.1. IDENTIFICACIÓN

Es recomendable que los accesos a los buzones estén completamente controlados y registrados, por ello se deberá usar el directorio activo para la creación de usuarios. Exchange Server 2016 facilita la creación de usuarios de directorio activo integrando en su propio panel de administración toda la creación y gestión del usuario sincronizándose automáticamente con el directorio activo de su organización.

Paso	Descripción
52.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
53.	Pulse sobre "Internet Explorer" en la barra de tareas. 

Paso	Descripción
54.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.
55.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
56.	Seleccione en la pestaña "destinatarios" en la opción de "buzones" un nuevo "Buzón del usuario". 

Paso	Descripción
57.	A continuación, documente los datos del nuevo buzón que desea crear, una vez documentado pulse sobre "Guardar".  **Nota:** También se pueden crear un buzón a un usuario existente en el directorio activo, en este ejemplo se crea un usuario nuevo con su correspondiente buzón.
58.	Una vez creado el nuevo usuario y buzón es posible modificar más características editándolo. Para ello seleccione el buzón que desea editar y pulse "Modificar". 

Paso	Descripción
59.	En la siguiente pantalla puede añadir todos los datos adicionales necesarios para su organización, para ello debe navegar por las diferentes opciones situados en el panel izquierdo. Para finalizar pulse sobre "Guardar". 

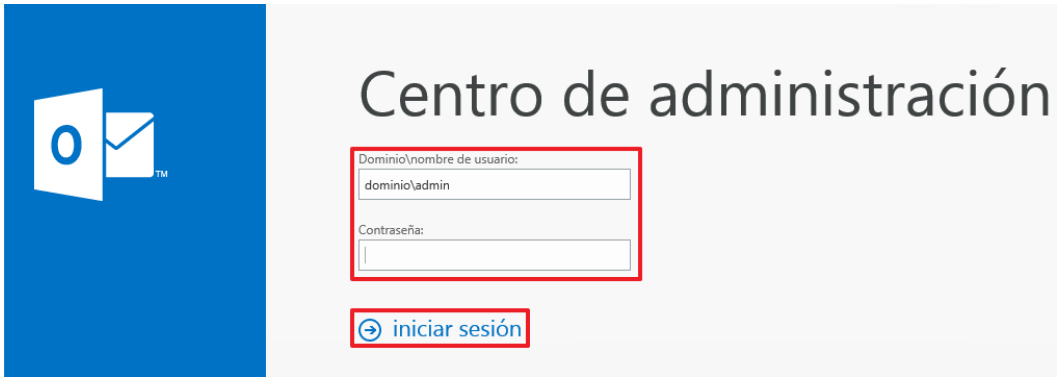
3.2. ASIGNACIÓN DE PERMISOS Y ROLES

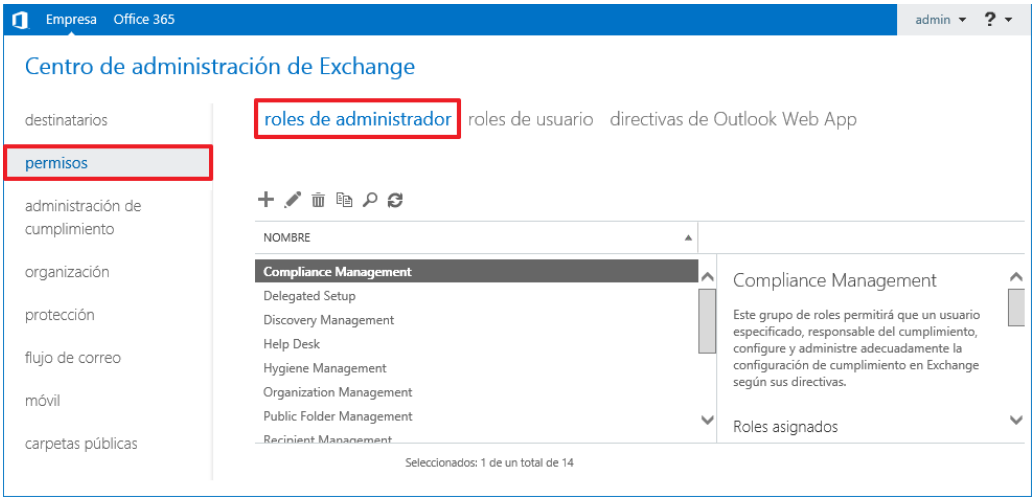
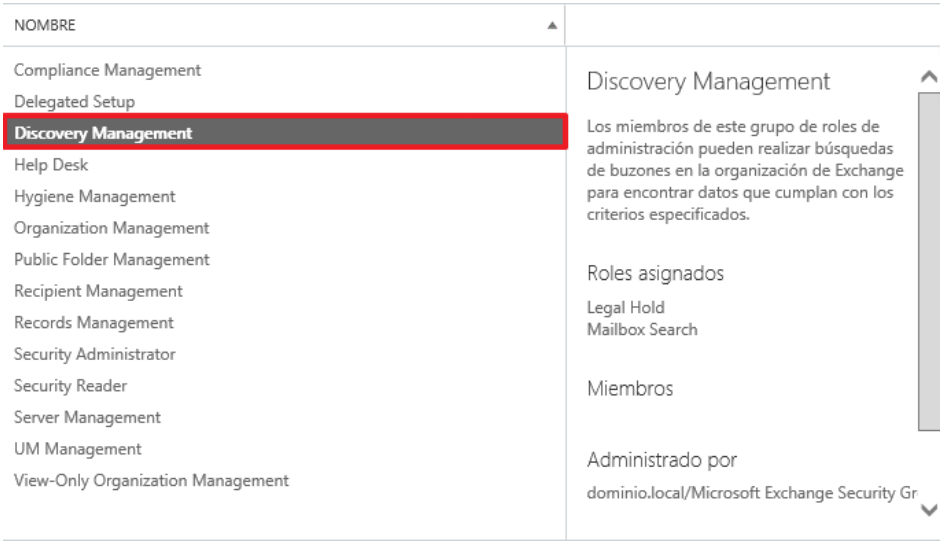
Antes de poder aplicar diferentes mecanismos de auditoría y conformidad, debe tener presente que determinadas funcionalidades requieren de la obtención de permisos específicos para la realización de las operaciones. La asignación de dichos permisos se basa en el modelo RBAC (Role Based Access Control). Dicho modelo tiene su base fundamental en la pertenencia a grupos y a la aplicación de directivas sobre dichos grupos.

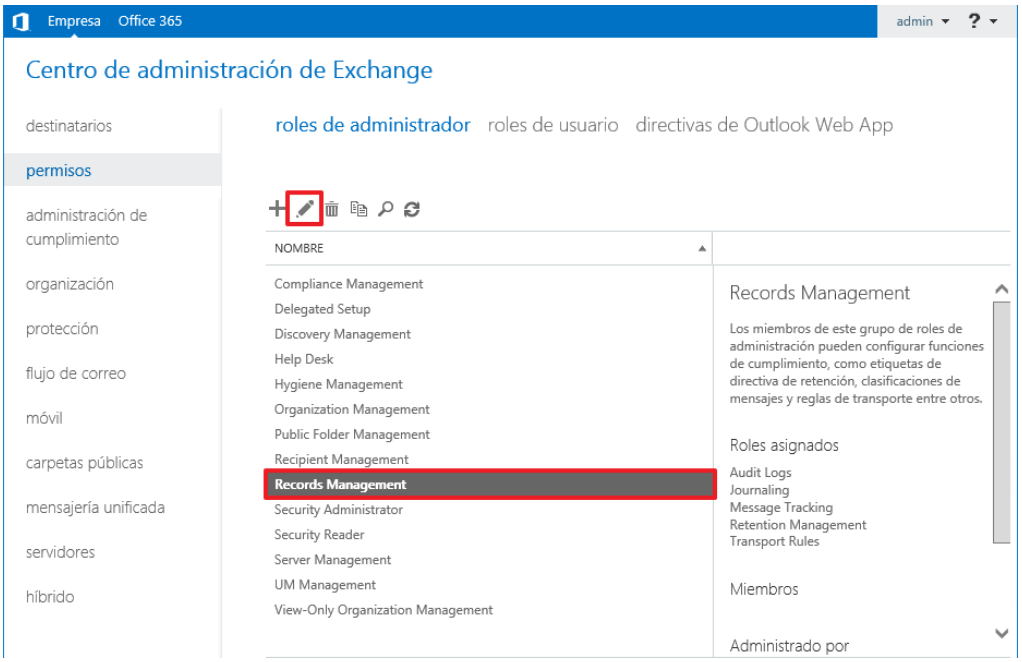
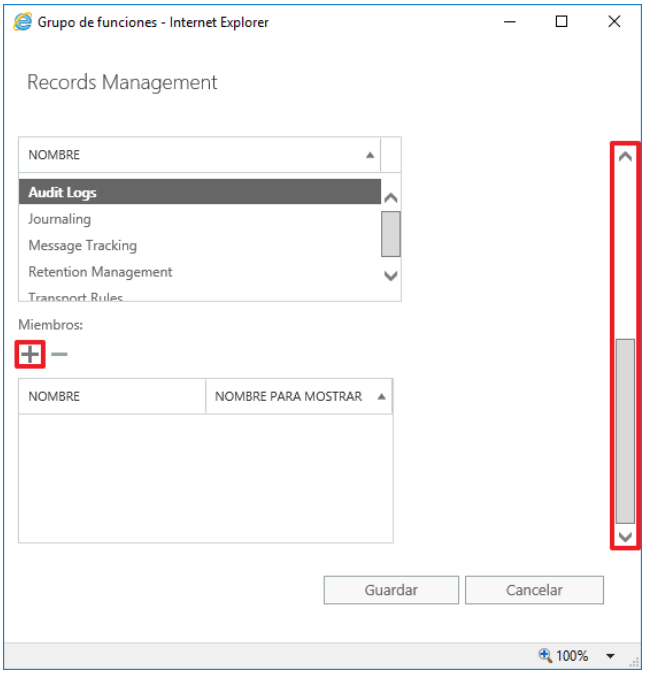
Así mismo, este modelo permite establecer una jerarquía de roles segregados, de tal forma que algunos usuarios de la organización pueden realizar tareas de administración del servidor, a la vez que otros pueden asumir la funcionalidad de auditores del sistema.

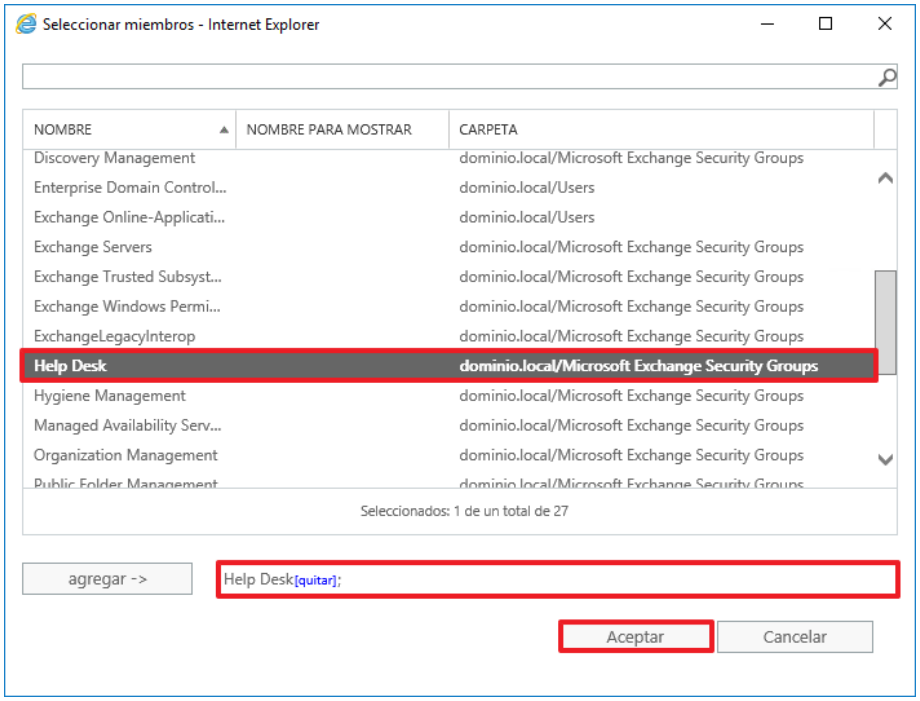
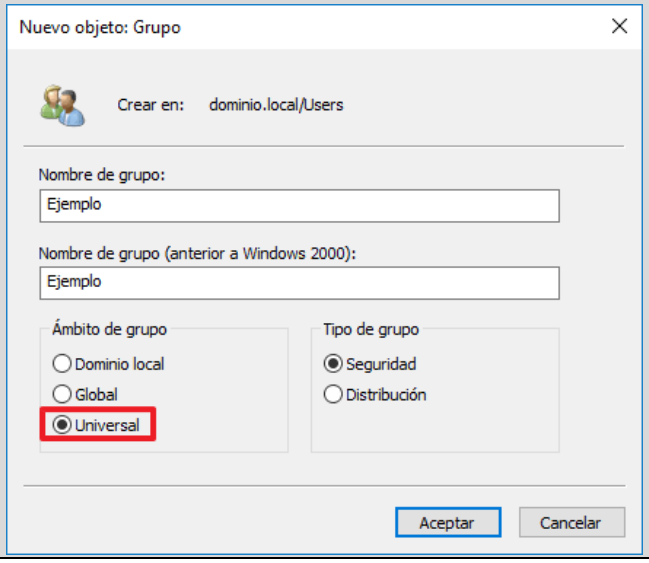
La administración de roles y permisos se puede realizar a través de la consola Web de administración (Exchange Control Panel) o bien a través de cmdlets de PowerShell. Para una mejor comprensión, este anexo mostrará cómo realizar dichas acciones a través del entorno gráfico vía Web.

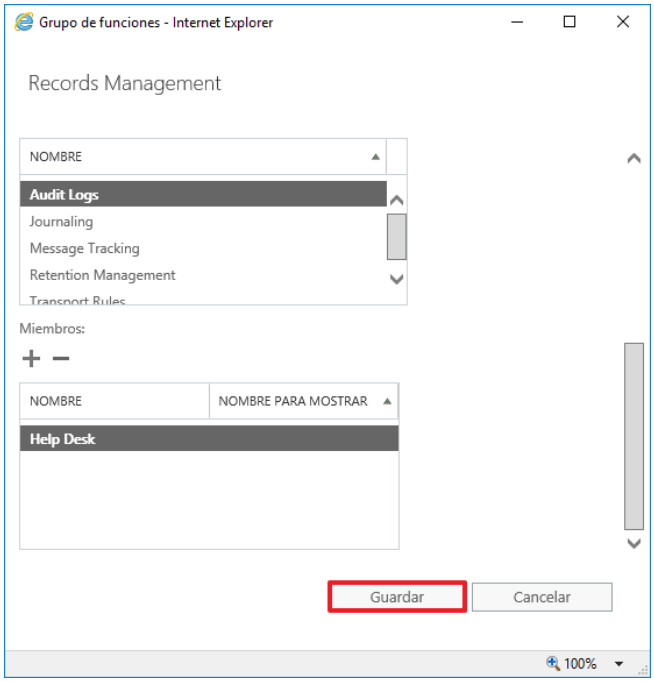
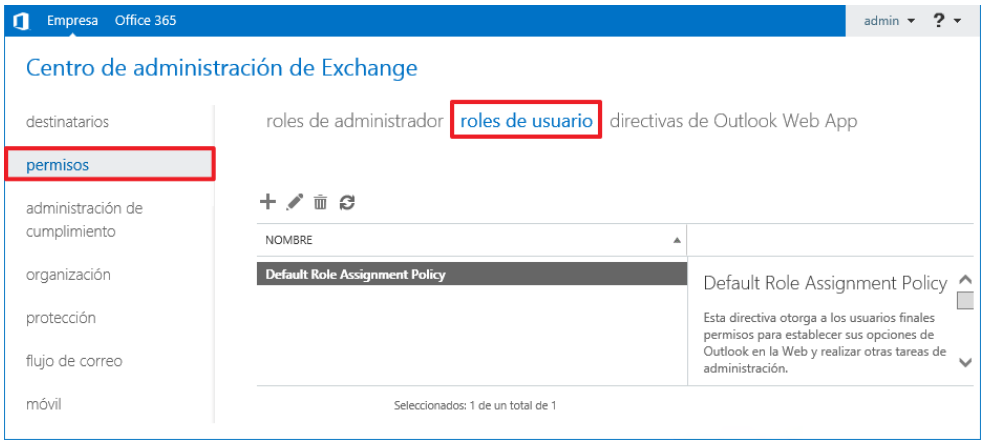
Nota: Si desea crear más información sobre la administración de roles y permisos visite la siguiente web: https://technet.microsoft.com/es-es/library/jj657511(v=exchg.150).aspx.

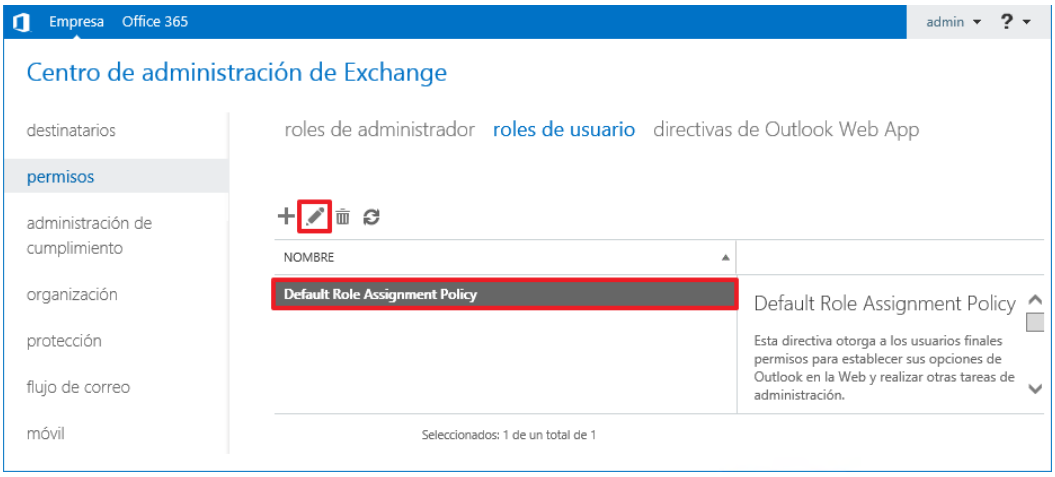
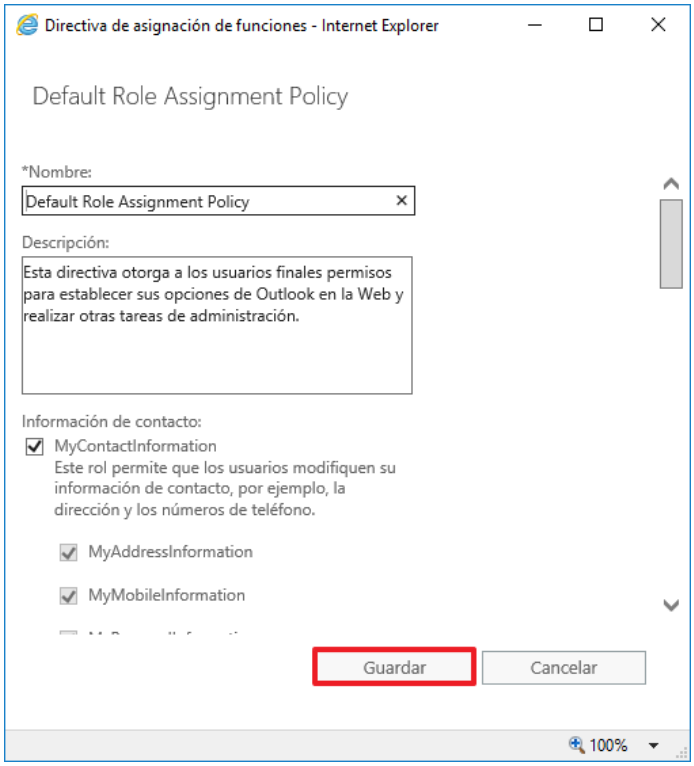
Paso	Descripción
60.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
61.	Pulse sobre "Internet Explorer" en la barra de tareas. 
62.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.
63.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".

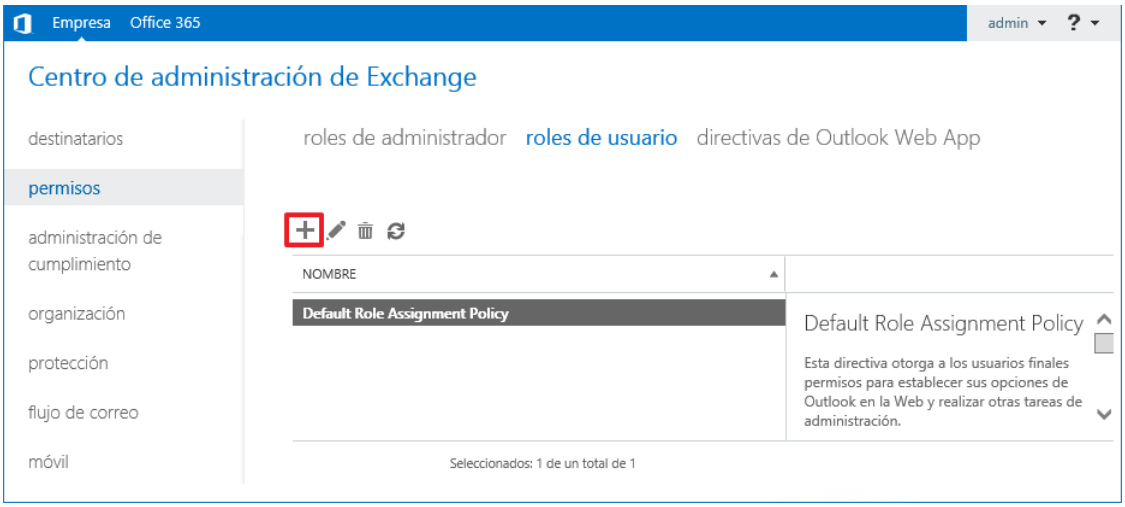
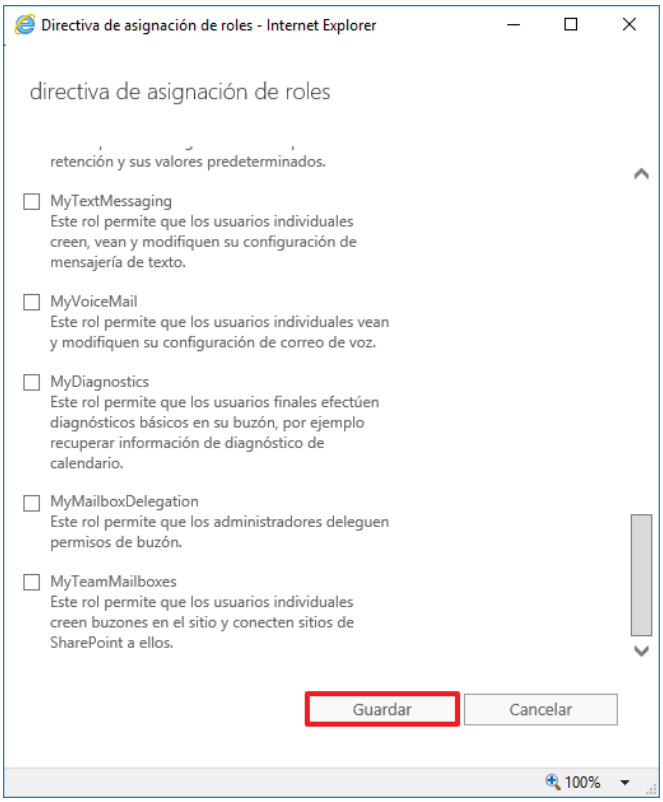
Paso	Descripción
64.	Seleccione el enlace "Permisos" para configurar los permisos RBAC.  **Nota:** Desde este menú se pueden asignar roles de administrador predeterminados a grupos nuevos o existentes en la organización, o también se pueden crear nuevos roles de administrador con permisos específicos.
65.	Por ejemplo, el rol denominado "Discovery Management" o administración de la detección tiene asignados los permisos necesarios para trabajar con la retención legal, así como la suspensión y exhibición de datos electrónicos. Estos permisos incluyen la realización de búsquedas de buzones en la organización para obtener datos que cumplan determinados criterios y la configuración de retenciones legales en los diferentes buzones de correo. 

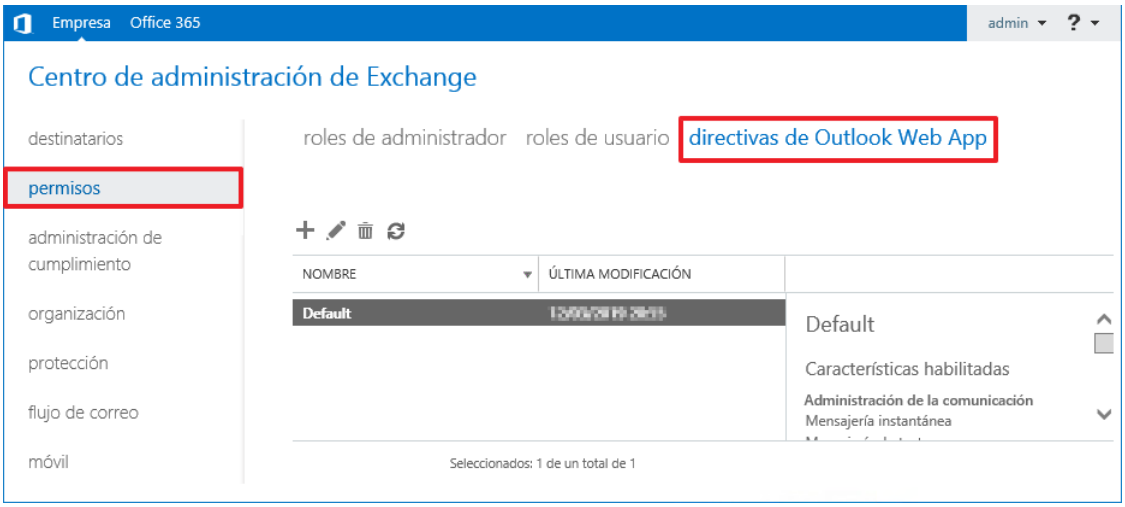
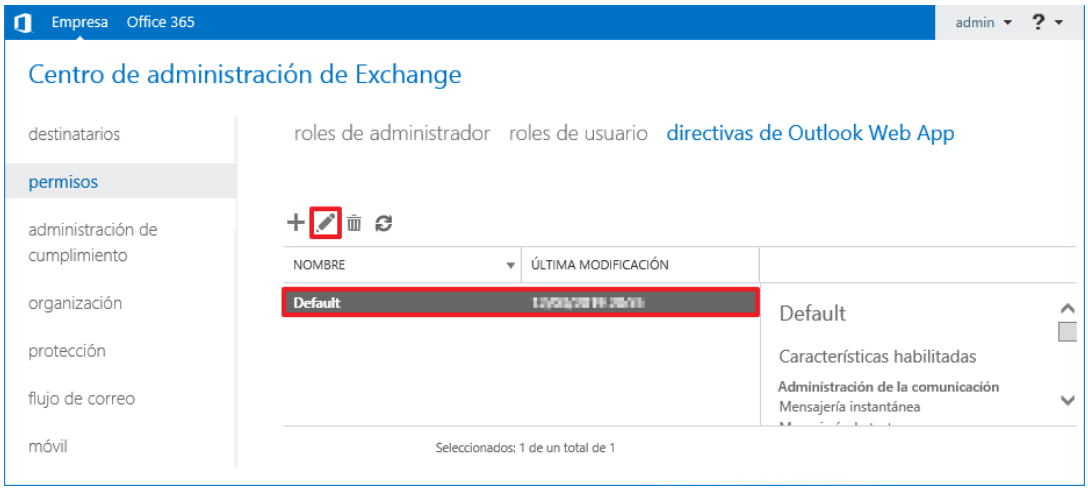
Paso	Descripción
66.	Por otro lado, el rol denominado "Records Management" o administración de registros, incluye otra serie de permisos asignados relativos a las capacidades de auditoría. A continuación, a modo de ejemplo, se va a asignar dicho rol a un grupo de seguridad de Directorio Activo. Para ello, seleccione el rol "Records Management" y pulse el botón "Modificar". 
67.	A continuación, en la sección "Miembros", podrá agregar un grupo de seguridad de Directorio Activo pulsando en el botón "+". 

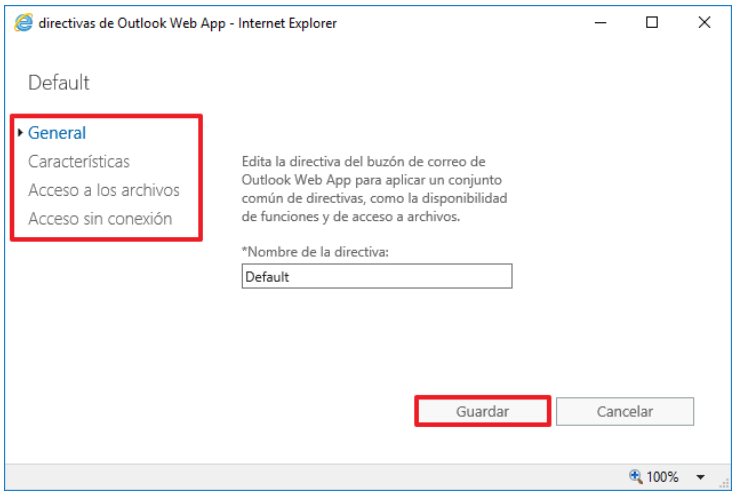
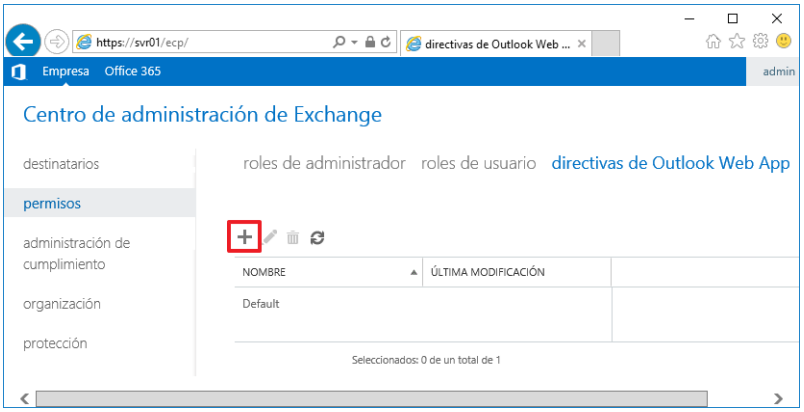
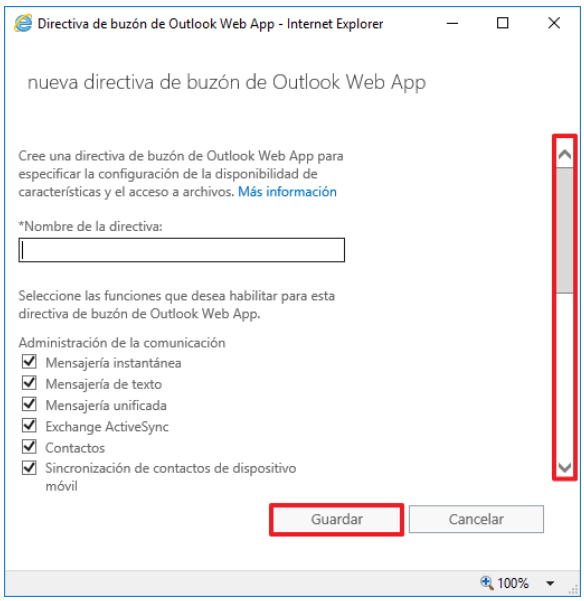
Paso	Descripción
68.	En la pantalla de selección, localice las cuentas de usuarios o grupos de seguridad universales que se desean añadir y pulse el botón "Agregar". Por ejemplo, seleccione el grupo "Help Desk" y pulse en el botón "agregar" y "aceptar".  **Nota:** Para que los grupos de seguridad del Directorio Activo aparezcan en esta ventana de selección, deben ser grupos universales. Los grupos globales o locales no serán visibles. 

Paso	Descripción
69.	A continuación, pulse sobre el botón "Guardar" para hacer efectivos los cambios. 
70.	A continuación, también puede crear grupos de roles de usuario para ello diríjase a la pestaña "permisos" y después a la pestaña "roles de usuario". 

Paso	Descripción
71.	Es posible modificar el grupo de roles de usuario por defecto, pulse sobre el grupo "Default Role Assignment Policy" y a continuación, seleccione "Modificar". 
72.	A continuación, se pueden modificar los campos que sean necesarios para adaptarlos a los requerimientos de su organización y pulse "Guardar". 

Paso	Descripción
73.	Del mismo modo es posible crear un grupo de roles de usuario nuevo, para ello seleccione la pestaña "roles de usuario" pulse sobre la opción nuevo o "+". 
74.	A continuación, cumplimente los campos en función de las necesidades de su organización y pulse "Guardar". 

Paso	Descripción
75.	Del mismo modo puede cambiar las directivas de Outlook Web App, para ello diríjase a la opción "directivas de Outlook Web App". 
76.	A continuación, seleccione la opción que viene creada por defecto, para ello seleccione "Default" y pulse el icono "Modificar".  **Nota:** El valor predeterminado de directiva de buzón de correo de Outlook Web App tiene todas las opciones habilitadas de forma predeterminada.

Paso	Descripción
77.	Cumplimente los campos en función de las necesidades de su organización y pulse "Guardar". 
78.	Si desea crear un grupo de directivas nuevo, debe pulsar sobre nuevo o "+". 
79.	Rellene los campos en función de las necesidades de su organización y pulse "Guardar". 

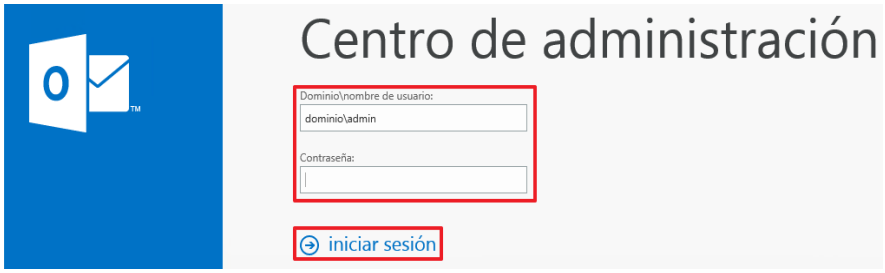
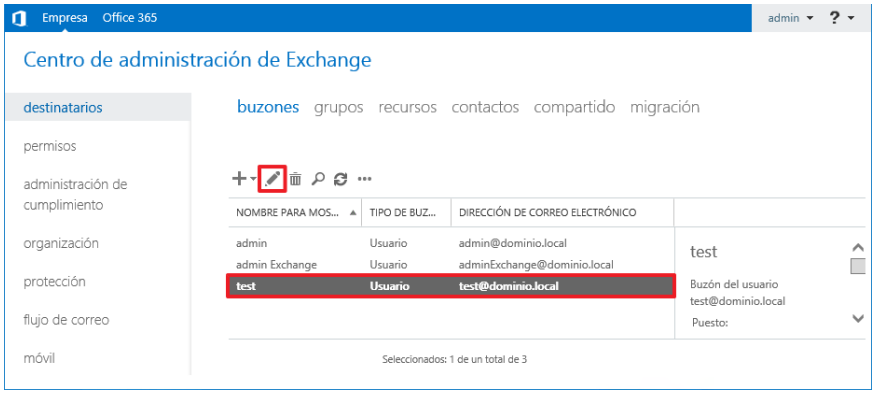
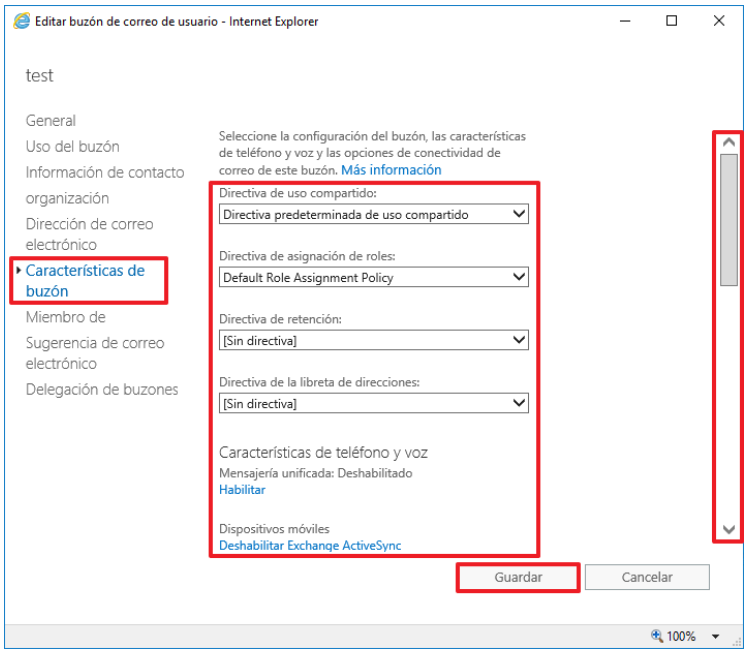
3.3. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

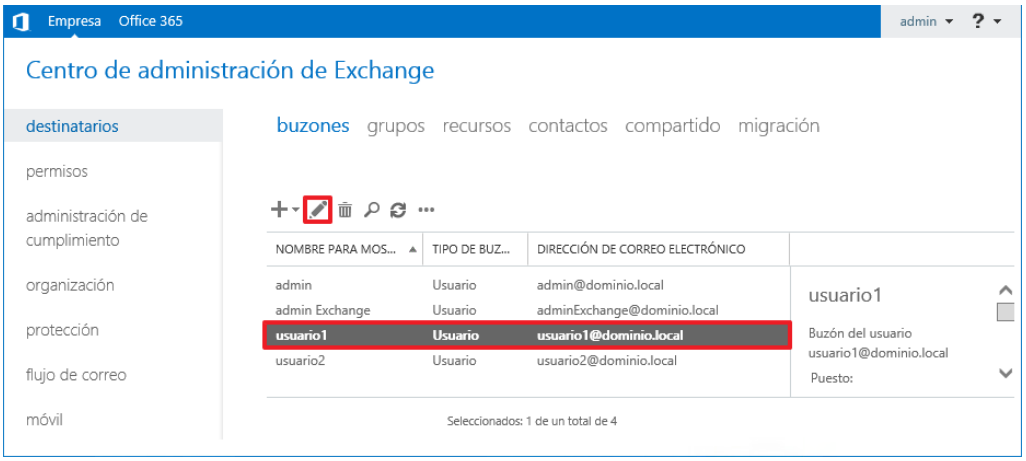
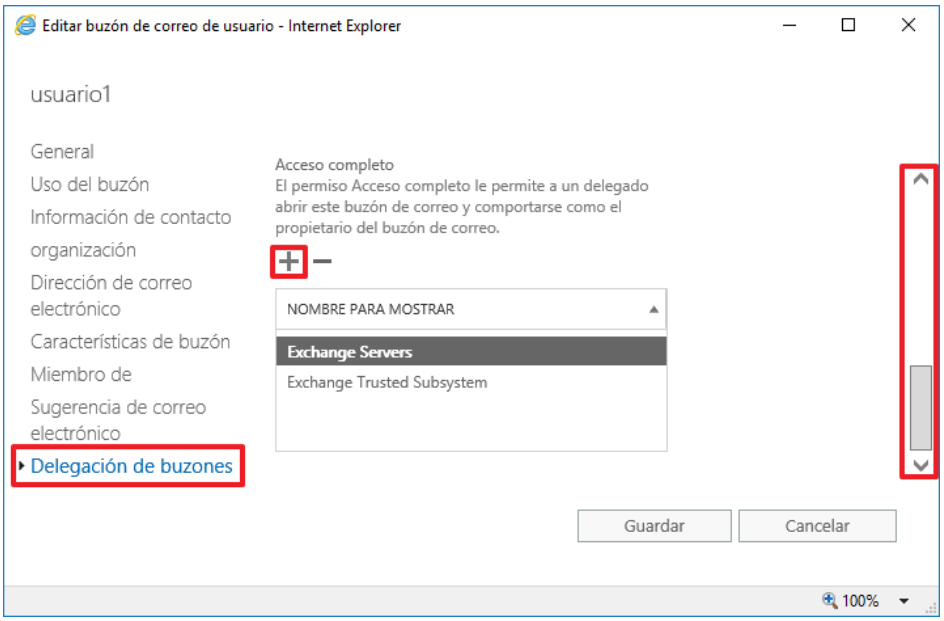
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional, es la mínima funcionalidad y mínima exposición evitando con ello posibles vulnerabilidades minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es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

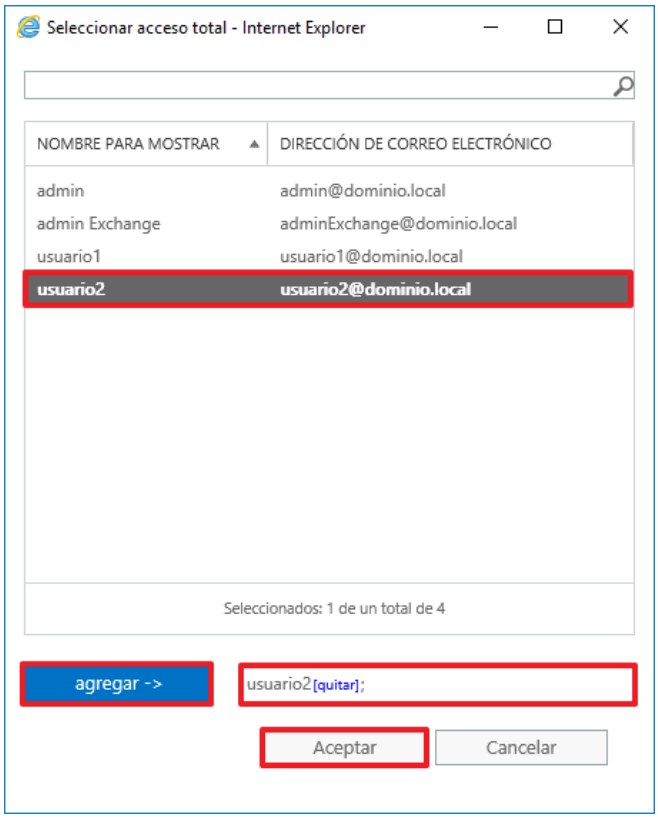
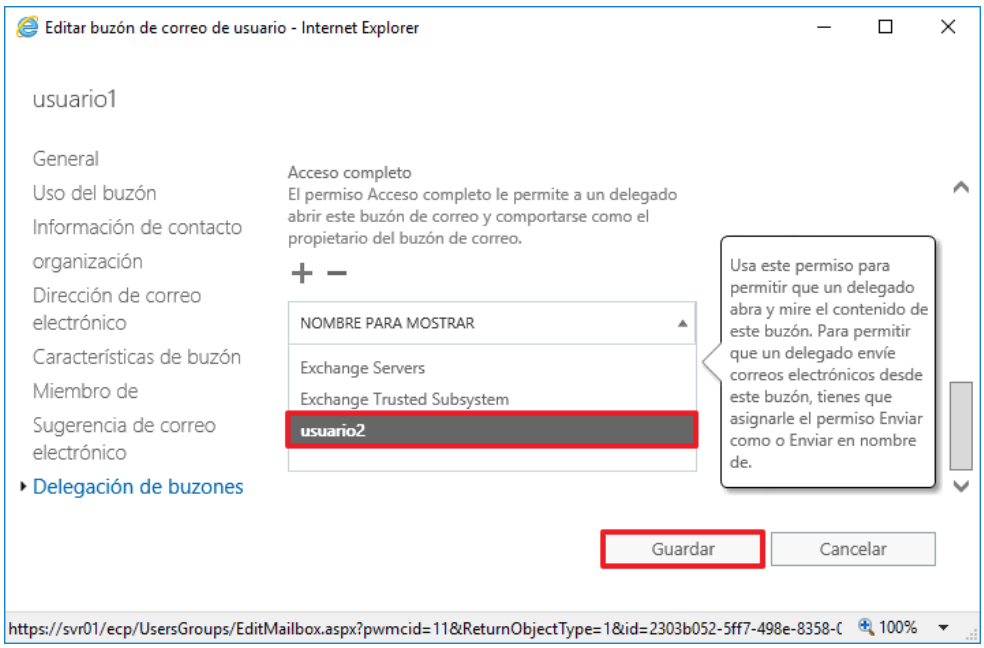
Microsoft Exchange Server 2016 instala por defecto las mínimas funcionalidades para el uso correcto de su producto, por lo que no es posible desinstalar características ya que conllevaría un mal funcionamiento del producto.

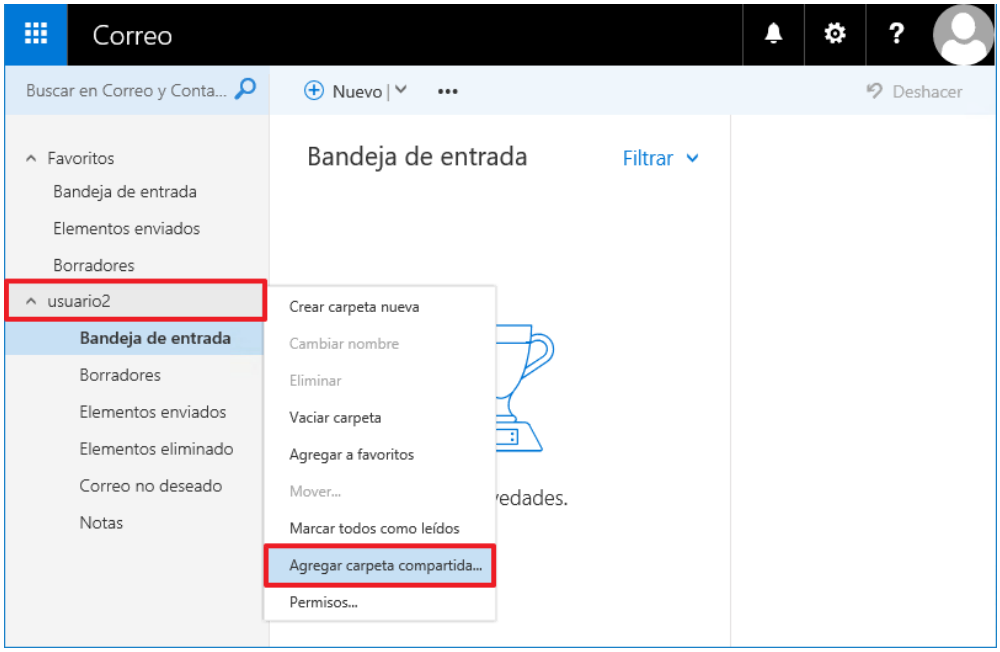
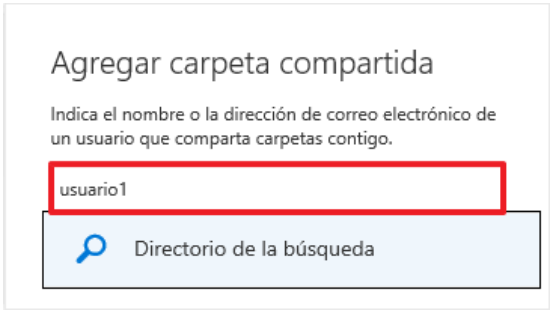
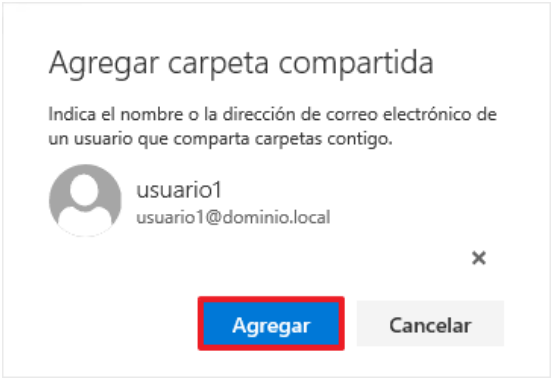
Microsoft Exchange Server 2016 por defecto deshabilita diferentes funcionalidades para aplicar seguridad en el entorno, por ejemplo, los servicios de POP3 e IMAP vienen deshabilitados por lo que si es necesario para su entorno deberá habilitarlo manualmente.

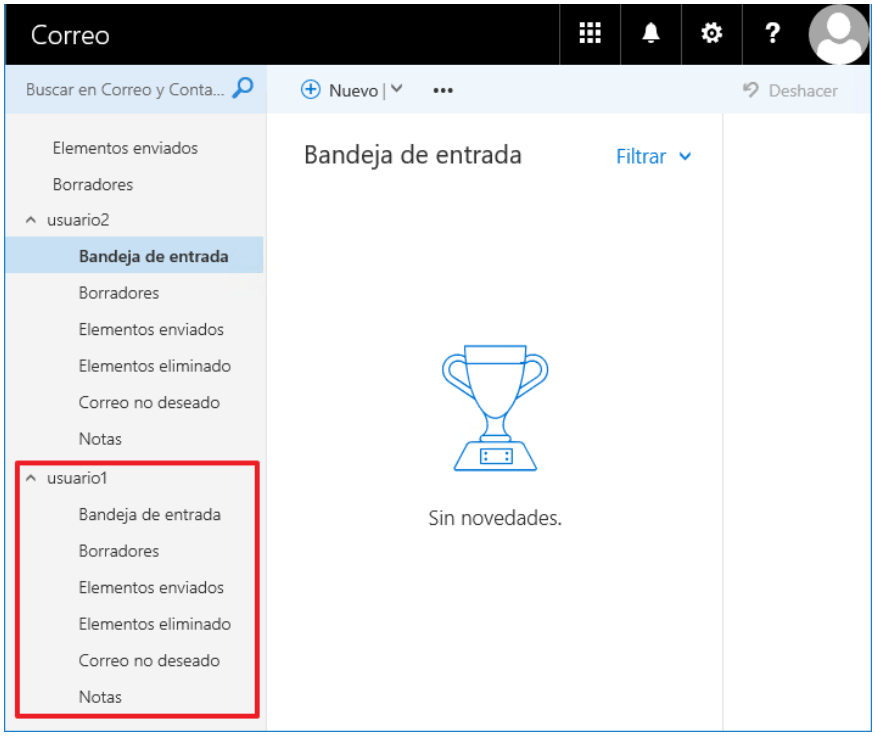
Paso	Descripción
80.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
81.	Pulse sobre "Internet Explorer" en la barra de tareas. 
82.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.

Paso	Descripción
83.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
84.	Seleccione el usuario o buzón en el que desea modificar alguna de las funcionalidades editándolo. Para ello seleccione el buzón que desea editar y pulse "Modificar".  **Nota:** En este ejemplo se usa la cuenta "test". Deberá adaptar los pasos de acuerdo a las necesidades de su organización.
85.	Localice en el menú lateral izquierdo, la opción de "Características de buzón" y seleccione la configuración de buzón según las necesidades de su organización. 

Paso	Descripción
86.	Una característica de seguridad configurable es la posibilidad que un usuario tenga acceso a un buzón de otro usuario, para ello se debe primero conceder los permisos necesarios para acceder al buzón. Seleccione el buzón al que desea acceder con otro usuario y pulse editar.  **Nota:** Para poder realizar este ejemplo se han creado previamente dos buzones, usuario1 y usuario2.
87.	A continuación, desplácese hacia abajo hasta localizar la característica "Acceso completo" dentro del menú "Delegación de buzones" y pulse el botón "agregar" o "+". 

Paso	Descripción
88.	Seleccione el usuario al que desea dar acceso al buzón, pulse "agregar ->" y "Aceptar". 
89.	Compruebe que se ha añadido al usuario dentro de "Acceso Completo". Para finalizar, pulse "Guardar". 

Paso	Descripción
90.	Para comprobar la correcta configuración, inicie sesión en el buzón del "Usuario2", pulse botón derecho sobre una carpeta, y seleccione "Agregar carpeta compartida...".  **Nota:** En este ejemplo se ha usado la cuenta de correo "Usuario2". Adapte estos pasos a los más convenientes para su organización.
91.	A continuación, escriba el usuario o el buzón que desee agregar. 
92.	Una vez seleccionado el usuario pulse "Agregar". 

Paso	Descripción
93.	Compruebe que tiene acceso al nuevo buzón agregado. 

3.4. MECANISMOS DE AUTENTICACIÓN

En Microsoft Exchange Server 2016 la autenticación básica establecida por defecto se realiza con usuario y contraseña gracias a la integración con el directorio activo de su organización asegurando que las contraseñas cumplan con los requisitos mínimos que se establecen en el ENS, por lo que se deben asegurar en la categoría básica del marco operacional unas claves seguras.

En la categoría básica del marco operacional del ENS se recomienda no usar claves concertadas, aunque si está permitido su uso.

En la categoría alta - DL del marco operacional del ENS se recomienda el uso de tarjetas inteligentes para el cual es necesario el uso del cifrado del nivel de sockets seguros (SSL), de manera predeterminada Outlook Web Access utiliza SSL por lo que si desea usar la autenticación mediante tarjeta inteligente deberá mantenerlo habilitado o habilitarlo en necesario, además deberá obtener y configurar un certificado de una entidad de certificación de confianza.

Nota: Si desea más información sobre como configurar Outlook Web Access para el uso de una tarjeta inteligente visite el siguiente sitio web: https://technet.microsoft.com/en-us/library/bb691090(v=exchg.80).aspx

3.5. CERTIFICADOS

Cuando se instala Microsoft Exchange Server 2016, se configura por defecto un certificado autofirmado en los servidores de buzones de correo. Este certificado autofirmado se usa para cifrar comunicaciones entre el servidor de acceso de cliente y el servidor de buzones de correo.

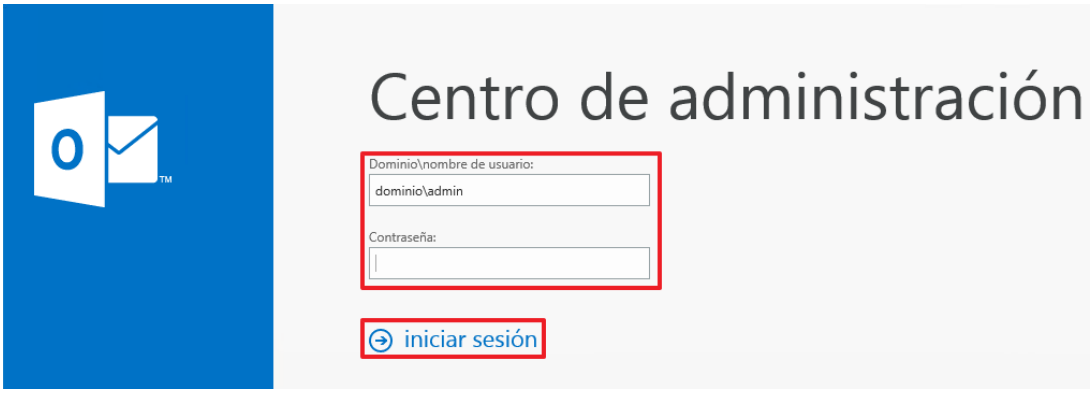
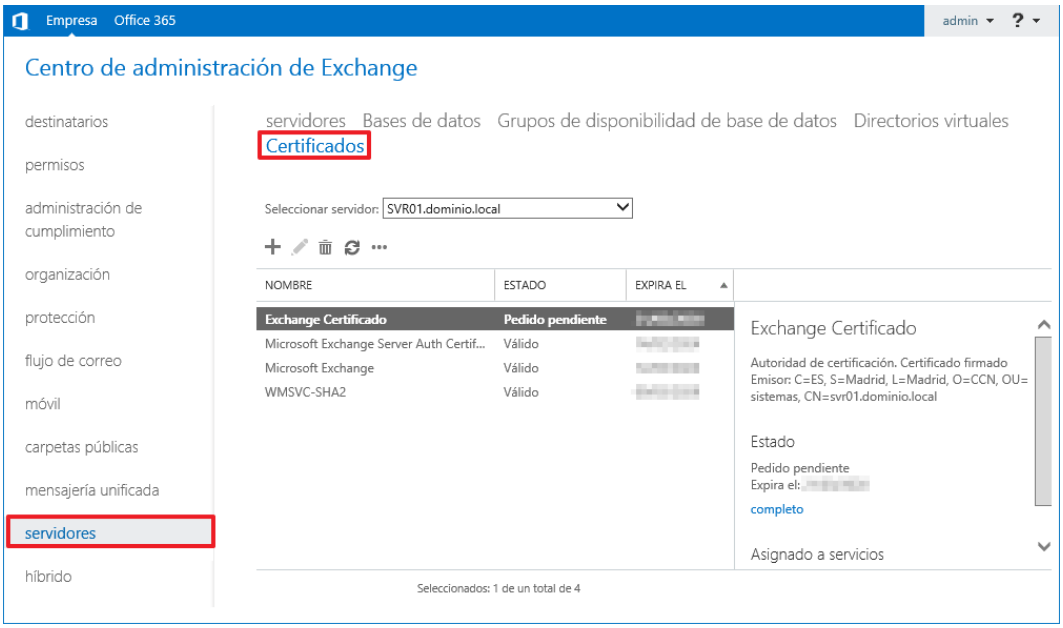
El servidor de acceso de cliente confía en el certificado autofirmado del servidor de buzones de correo automáticamente, así que no es necesario un certificado de terceros en el servidor de buzones de correo. Este certificado autofirmado permitirá que algunos protocolos de cliente usen SSL para sus comunicaciones. Exchange ActiveSync y Outlook Web App, pueden establecer una conexión SSL usando un certificado autofirmado.

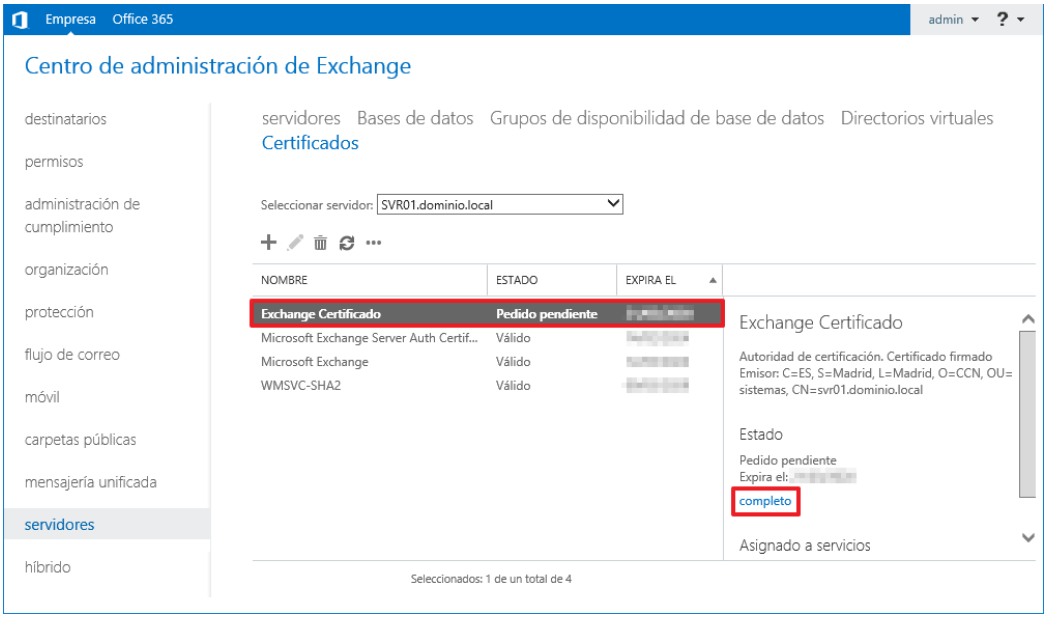
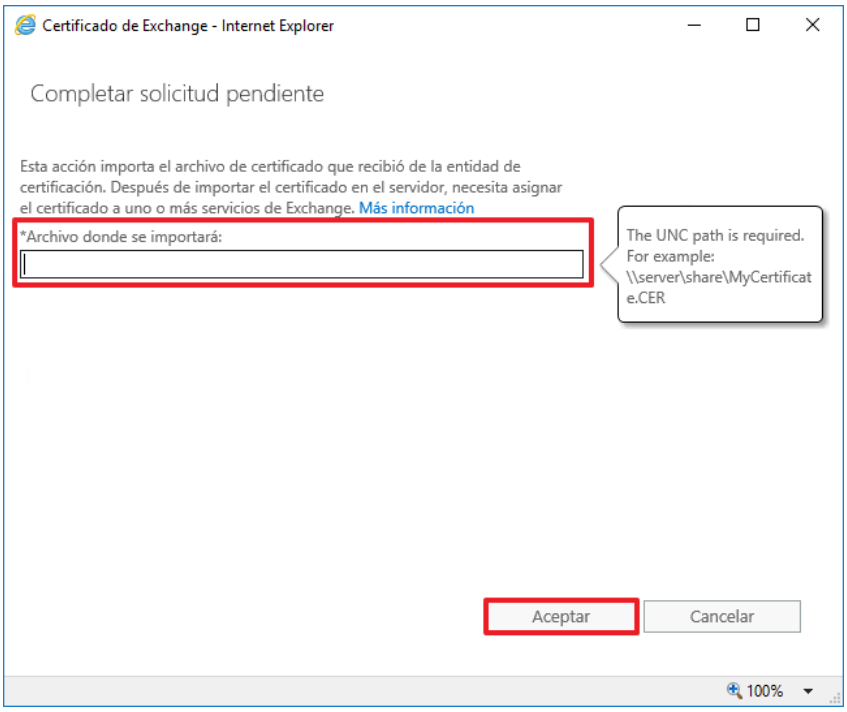
Sin embargo, el certificado autofirmado no es el más recomendable a la hora de implementar mecanismos de seguridad que requieran la confianza de clientes y usuarios ya que es relativamente sencillo suplantar la identidad de un certificado de estas características. Para evitar esto, se requiere la emisión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

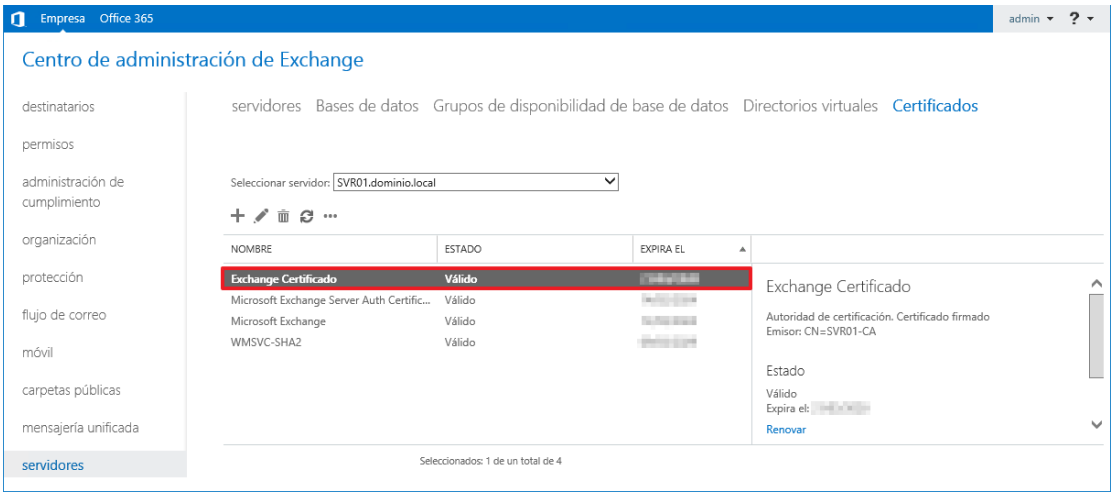
La implementación de certificados puede realizarse bien empleando certificados emitidos por una entidad certificadora que la organización haya implementado o bien por un certificado adquirido a una entidad certificadora de terceros como puede ser la FNMT (Fábrica Nacional de Moneda y Timbre).

A continuación, se muestra un ejemplo de cómo instalar un certificado emitido por una entidad certificadora autorizada, en este paso a paso se da por hecho que ya se ha solicitado un certificado a una entidad de certificación autorizada y se ha obtenido el certificado por lo que se explicara como instalarlo.

Paso	Descripción
94.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
95.	Pulse sobre "Internet Explorer" en la barra de tareas. 
96.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.

Paso	Descripción
97.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
98.	Seleccione en el menú lateral izquierdo la opción "servidores" y a continuación seleccione "Certificados".  **Nota:** En este ejemplo se da por hecho que se ha solicitado previamente un certificado emitido por una entidad certificadora autorizada para este servidor.

Paso	Descripción
99.	Seleccione el certificado el cual solicito previamente, y se encuentra en estado "Pedido pendiente". Pulse en el lateral derecho de la pantalla sobre "completo" para finalizar la instalación del certificado. 
100.	A continuación, seleccione el certificado .cer obtenido y pulse sobre "Aceptar". 

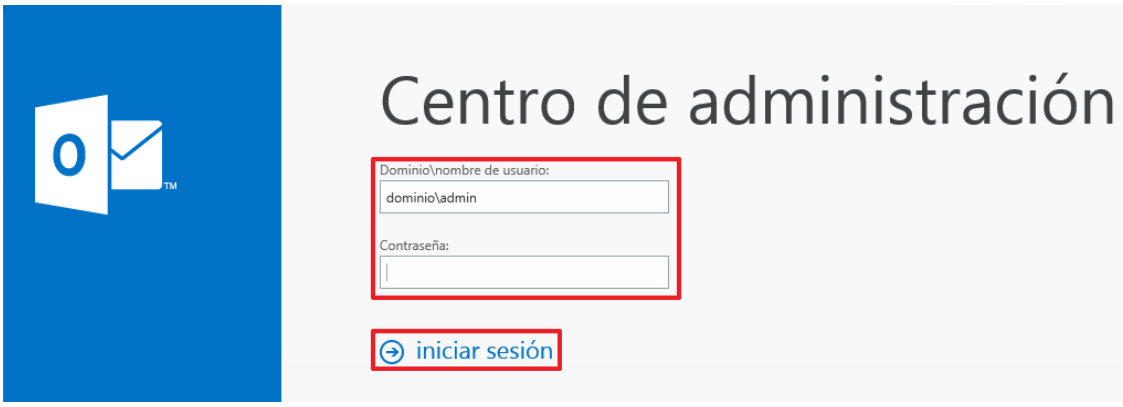
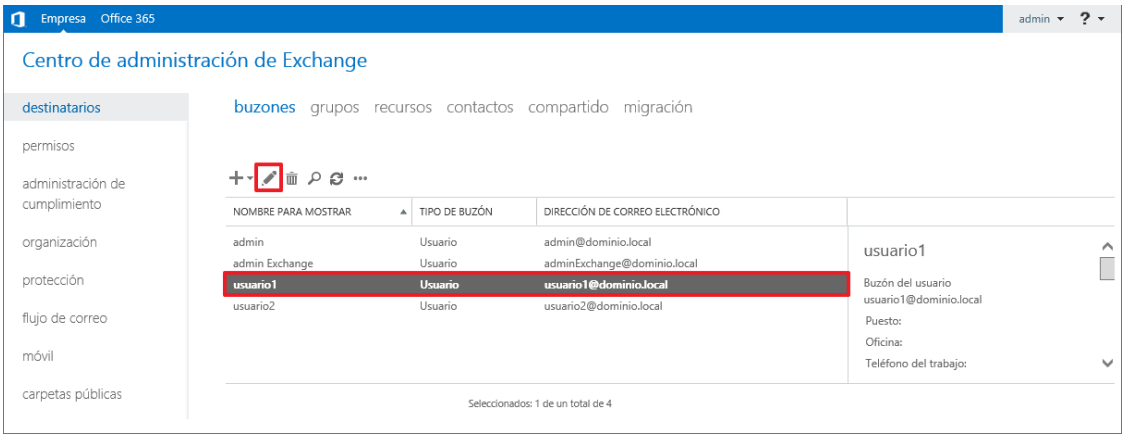
Paso	Descripción
101.	Compruebe que el estado del certificado instalado es válido y está asignado a los servicios que solicitó previamente. 

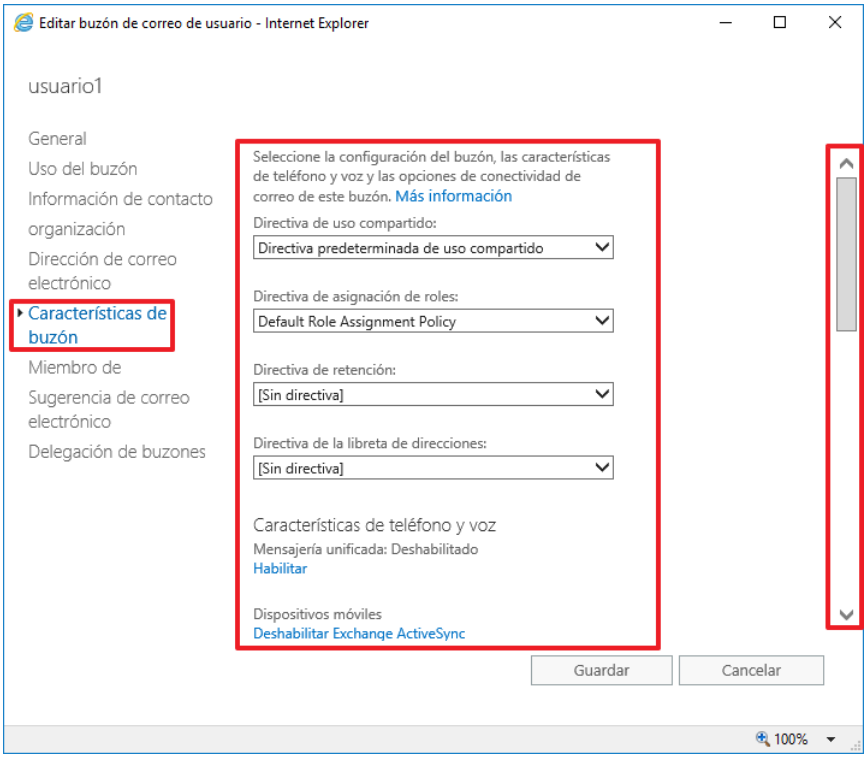
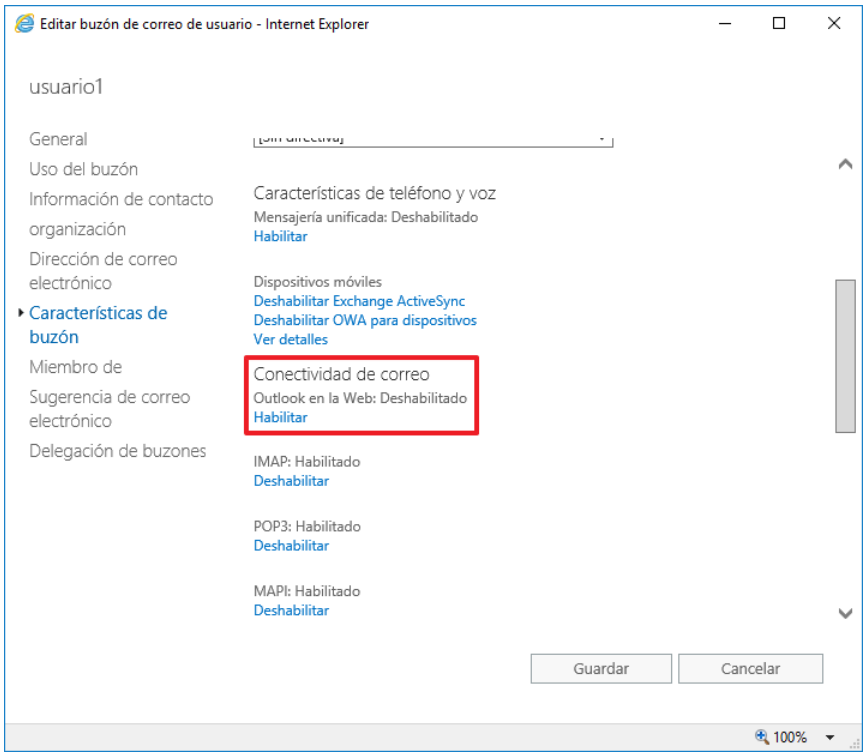
3.6. CONFIGURACIÓN DE SEGURIDAD

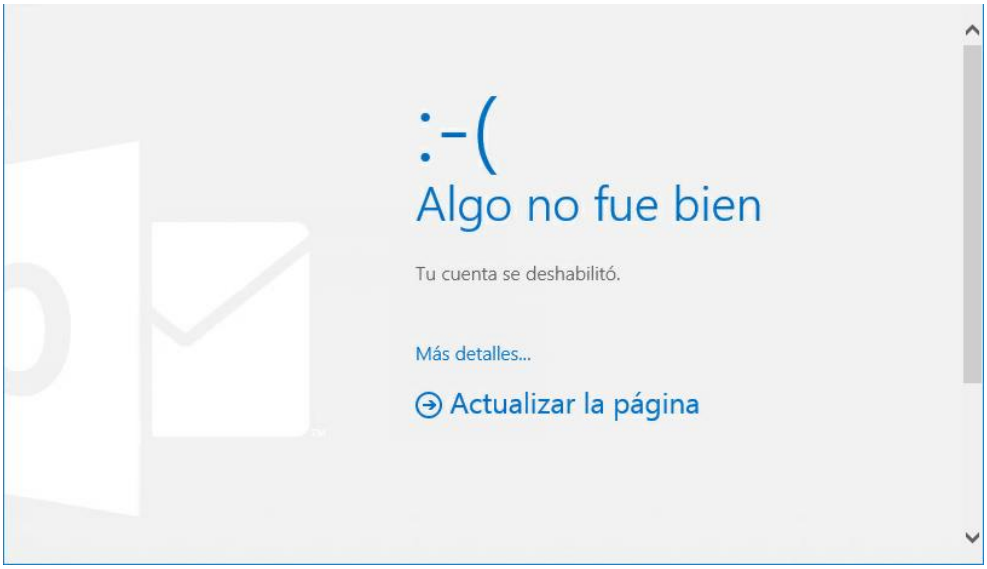
Microsoft Exchange Server 2016 instala POP3 e IMAP por defecto, pero los servicios se encuentran deshabilitados por lo que si es necesario su uso para su organización deberá habilitarlos manualmente.

En esta guía se va a usar el ejemplo de cómo deshabilitar una funcionalidad de Microsoft Exchange Server 2016 como principio de mínima funcionalidad y mínima exposición, deshabilitando la conectividad de correo Outlook Web App para aquellos buzones que no van a hacer uso de esta funcionalidad, limitando con ello, la exposición y aumentando la seguridad de la organización.

Paso	Descripción
102.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
103.	Pulse sobre "Internet Explorer" en la barra de tareas. 

Paso	Descripción
104.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.
105.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
106.	Seleccione el usuario o buzón en el que desea modificar alguna de las funcionalidades editándolo. Para ello seleccione el buzón que desea editar y pulse "Modificar". 

Paso	Descripción
107.	A continuación, seleccione del menú lateral izquierdo la opción de "Características de buzón" y seleccione la configuración de buzón según las necesidades de su organización. 
108.	Para realizar este ejemplo se ha deshabilitado la conectividad de correo: Outlook Web App, en el "usuario1" creado en los pasos anteriores. 

Paso	Descripción
109.	Para comprobar el funcionamiento, al intentar acceder al buzón usando la funcionalidad de OWA, https://nombre_servidor/owa, devuelve un error indicando que la cuenta esta deshabilitada. 

3.7. TAREAS DE MANTENIMIENTO

El fabricante de Microsoft Exchange Server 2016 publica periódicamente una serie de actualizaciones acumulativas que corrigen nuevas vulnerabilidades detectadas, dichas actualizaciones deben ser instaladas para cumplir con el ENS.

Microsoft Exchange Server 2016 no se actualiza automáticamente por lo que para actualizar el producto deberá descargar manualmente las actualizaciones de la página del fabricante.

Para el cumplimiento del ENS es recomendable realizar todas las tareas de actualización previamente en un entorno de test controlado que refleje el entorno de producción de su organización.

Antes de proceder a realizar una actualización acumulativa de Microsoft Exchange Server 2016, es recomendable realizar un backup previo del estado de los controladores de Active Directory, del rol de Mailbox (backup completo de las bases de datos) y del Client Access (Backup del IIS), además se tendrá que tener en consideración posibles personalizaciones del código por ejemplo de la interfaz gráfica del Outlook Web App el cual deberá ser respaldado para no sufrir pérdidas durante la instalación de la actualización.

Nota: Si desea obtener más información sobre las actualizaciones acumulativas de Microsoft Exchange Server 2016 visite el sitio web: https://technet.microsoft.com/es-es/library/hh135098(v=exchg.150).aspx.

3.8. REGISTRO DE ACTIVIDAD

Con la aplicación del ENS para la categoría básica sobre Exchange Server 2016 quedará registrado el uso del sistema para poder detectar y reaccionar a cualquier fallo accidental o deliberado, quedando registrado en el sistema quien realiza la actividad, cuando y sobre qué información con el fin de detectar anomalías o intentos frustrados de acceso a información no autorizada.

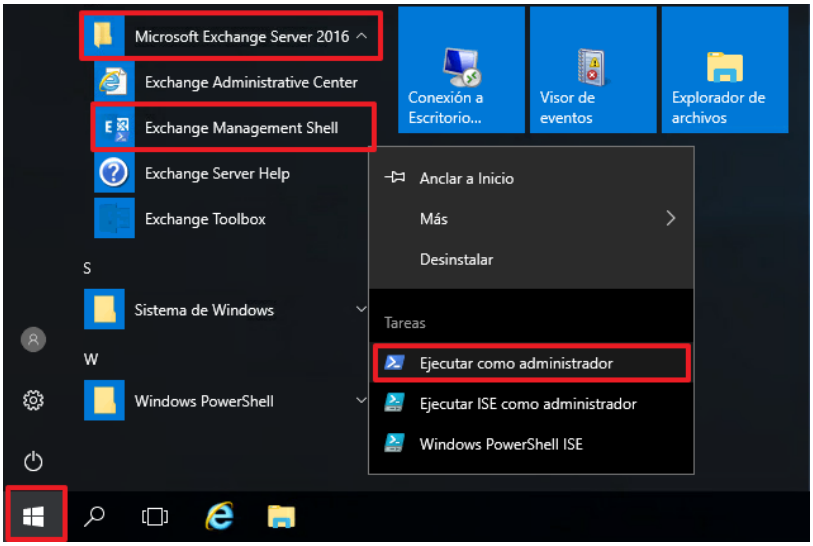
Es recomendable que la ubicación de los registros sea diferente a la del sistema además de tener limitado el acceso únicamente a los usuarios autorizados.

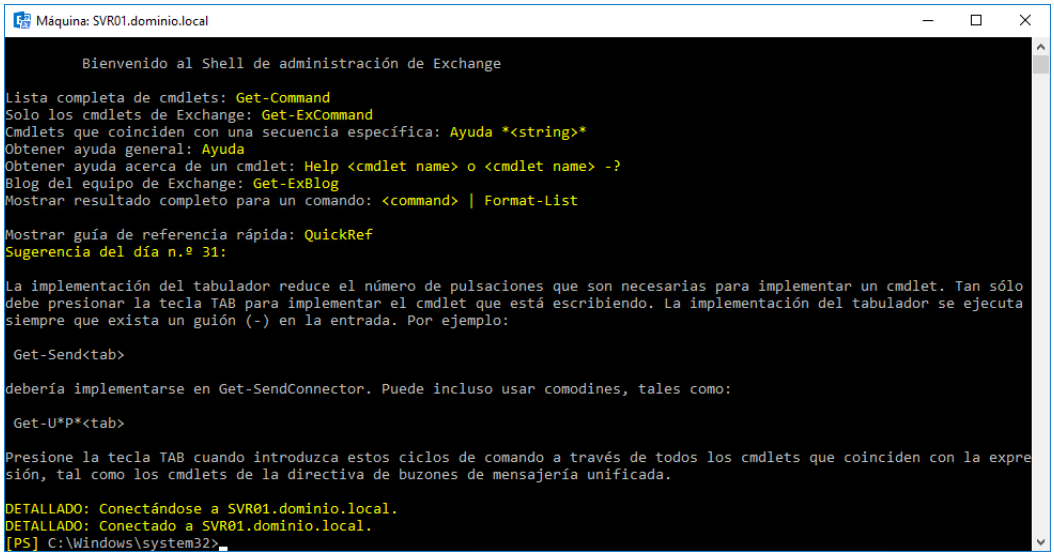
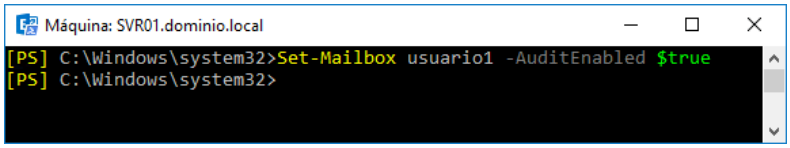
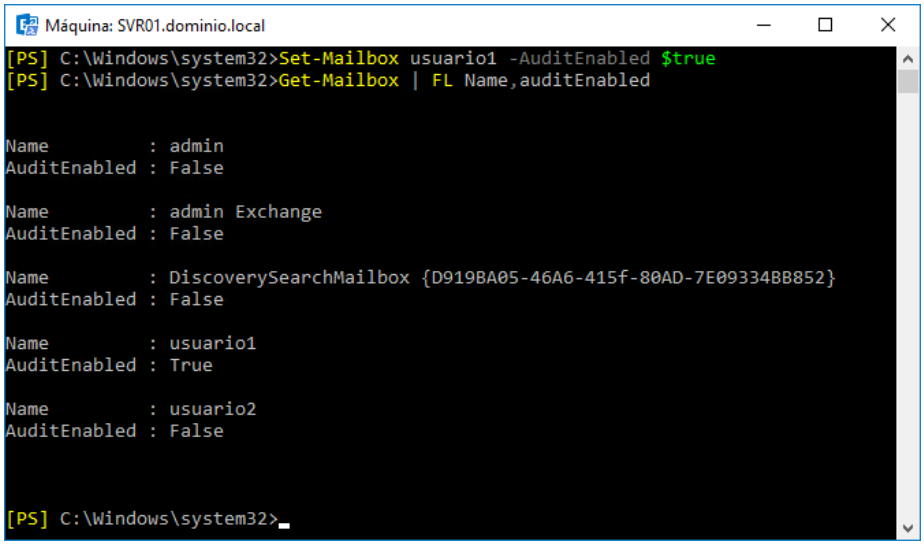
Mediante el registro de auditoría de buzón, se puede registrar el acceso y controlar los inicios de sesión a los buzones de correo por parte de sus propietarios, delegados (incluidos los administradores con permisos de acceso total al buzón) y administradores.

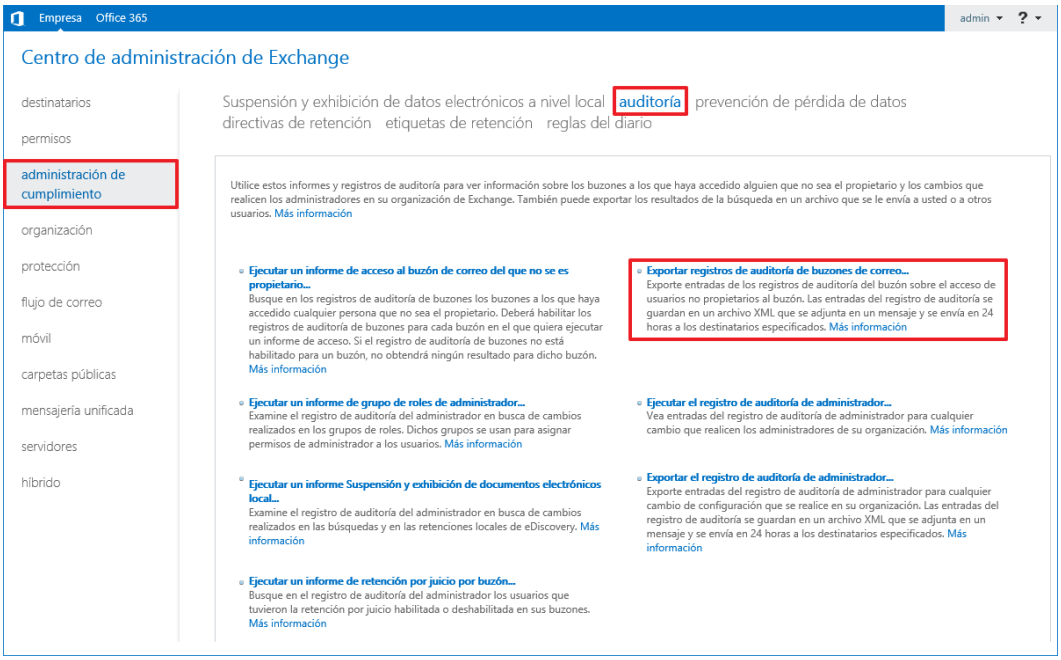
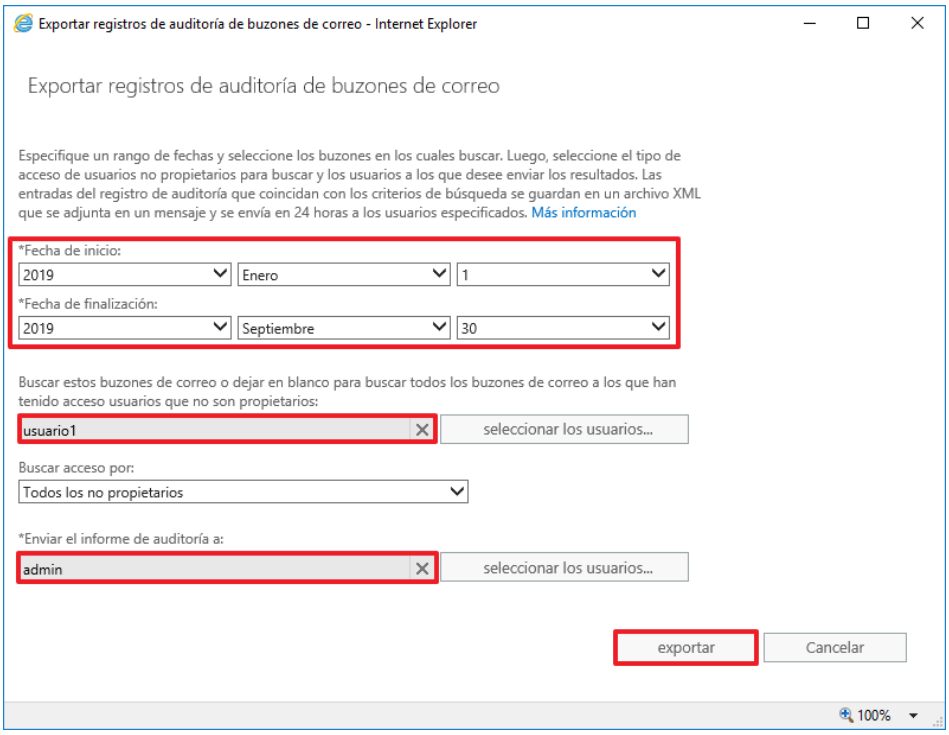
La auditoría de las acciones del propietario del buzón puede generar una gran cantidad de entradas en el registro de auditoría, por lo que se encuentra deshabilitada de forma predeterminada. Se recomienda activar solo la auditoría de algunas acciones específicas necesaria para cumplir con los requisitos comerciales o de seguridad.

Cuando un buzón de correo tiene habilitada la auditoría, Microsoft Exchange Server 2016 guarda la información de accesos al buzón y los elementos del buzón en el registro de auditoría de buzones de correo, siempre que un usuario que no sea el propietario obtenga acceso al buzón de correo.

Cada entrada de registro incluye información acerca de quién tuvo acceso al buzón y en qué momento, así como las acciones realizadas por el usuario que es no propietario y si la acción se realizó correctamente.

Paso	Descripción
110.	Inicie sesión en el servidor miembro donde está instalado Microsoft Exchange Server 2016 con un usuario con permisos de administrador.
111.	Pulse sobre el menú inicio despliegue la carpeta "Microsoft Exchange Server 2016" y pulsando con botón derecho en "Exchange Management Shell" seleccione "Ejecutar como administrador".  **Nota:** El sistema le solicitará elevación de privilegios.

Paso	Descripción
112.	A continuación, se mostrará la siguiente ventana. 
113.	Una vez conectado al Shell, ejecute la siguiente sintaxis. – Set-Mailbox <identity> -AuditEnabled $true  **Nota:** En este ejemplo se habilita la auditoría para el buzón de "usuario1".
114.	Para conocer los buzones donde se encuentra habilitada la auditoria, se puede ejecutar el siguiente cmdlet. – Get-Mailbox | FL Name,auditEnabled 

Paso	Descripción
115.	Es posible exportar los registros de auditoría de buzones desde la consola Web de administración de Exchange desde el menú "administración de cumplimiento" seleccionando la opción "Auditoría", tal y como se ha podido observar en el punto anterior.  **Nota:** Exchange puede tardar hasta 24 horas en generar el informe y enviarlo al destinatario seleccionado
116.	Deberá indicar el intervalo de fechas, los buzones en dónde realizar la búsqueda y el buzón de destino del informe. 

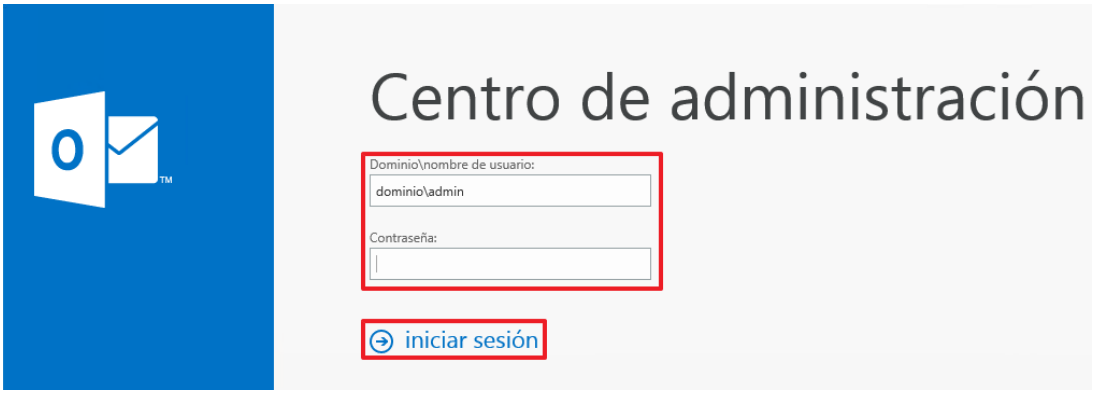
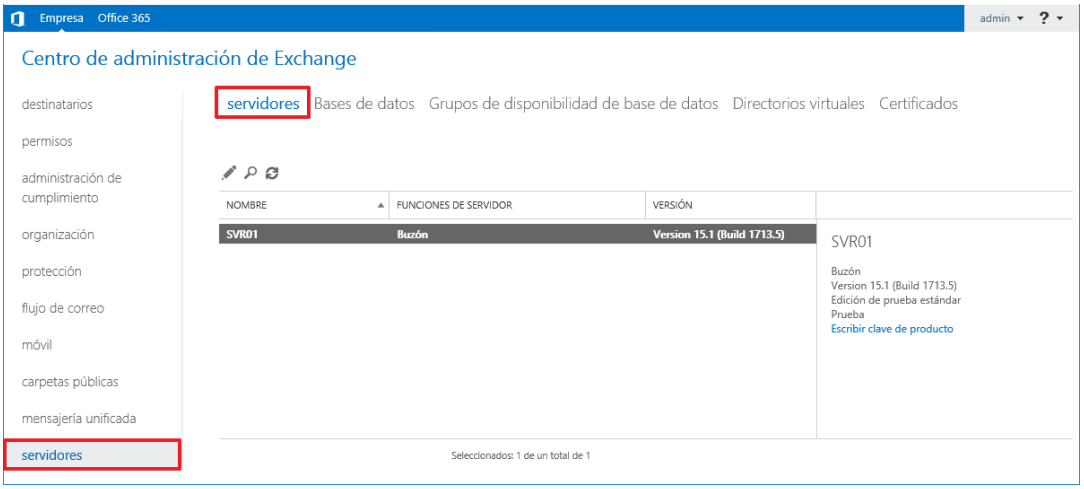
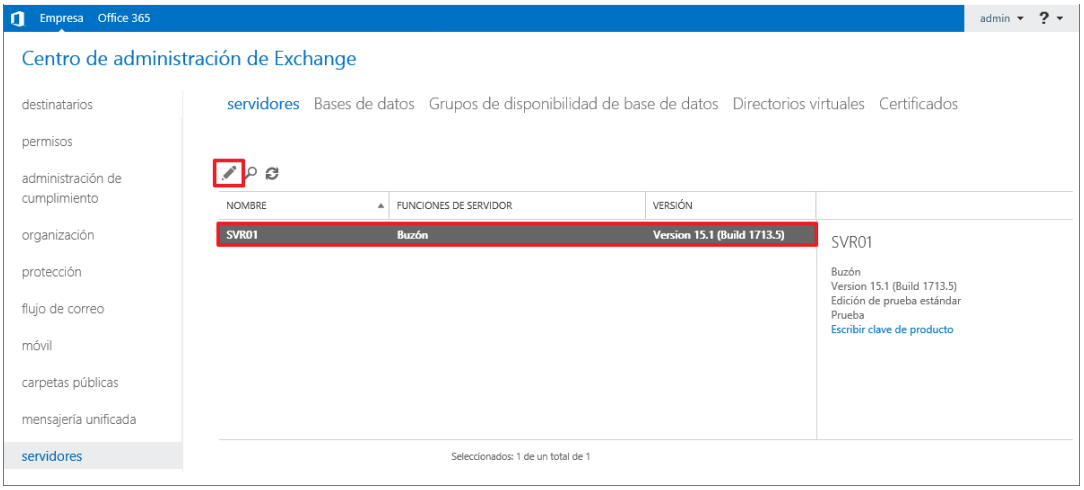
Paso	Descripción
117.	El resultado lo recibirá en su buzón el usuario especificado en la ventana de exportación de registros de auditoría. **Nota:** Debe tener en consideración que, si visualiza el informe desde Outlook Web App, de forma predeterminada se bloquea el acceso a los ficheros ".xml". Si quiere permitir que en Outlook Web App sean accesibles los ficheros ".xml", consulte la información que proporciona Microsoft en el siguiente enlace: https://technet.microsoft.com/es-es/library/jj150552(v=exchg.150).aspx.

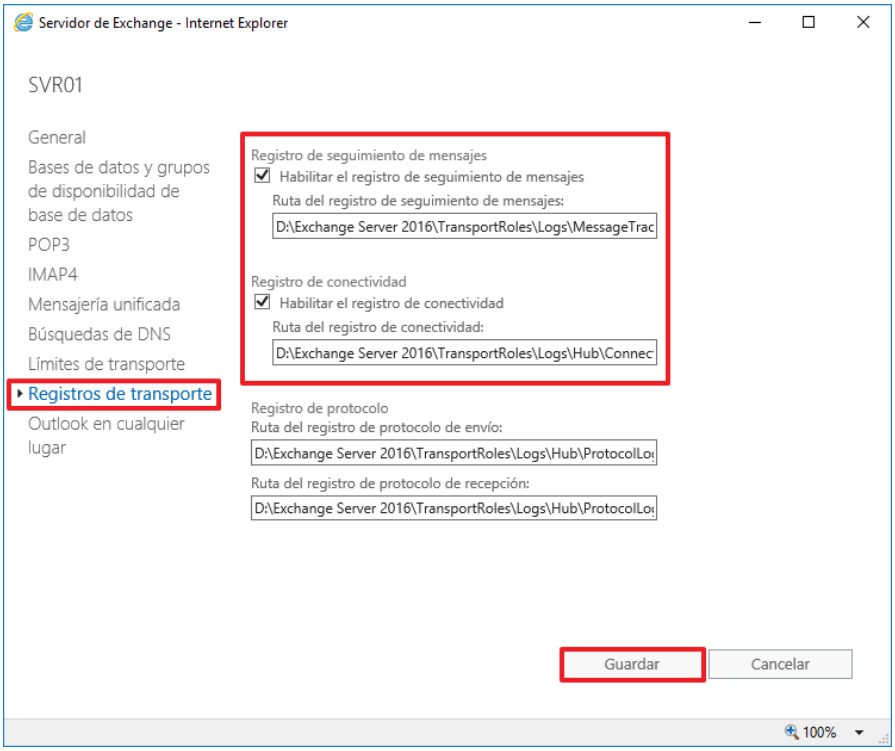
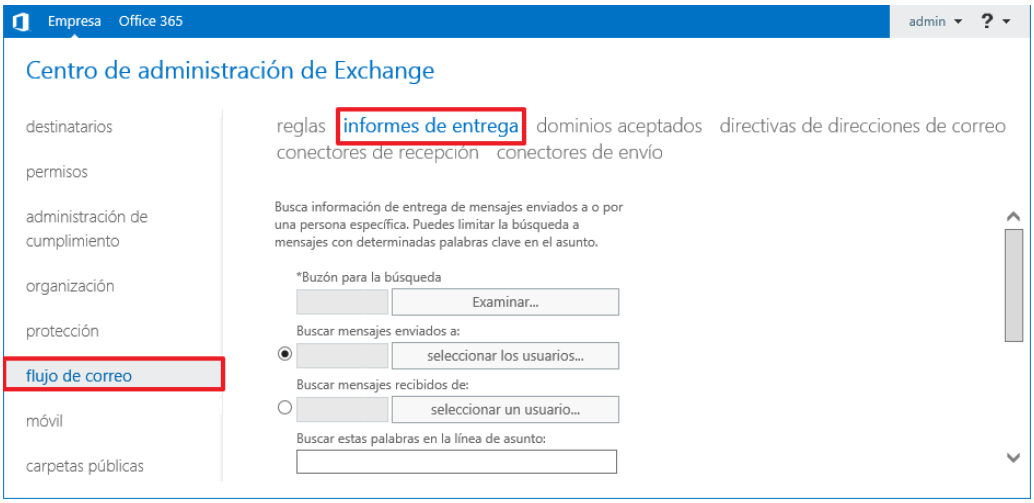
3.9. REGISTRO DE SEGUIMIENTO DE MENSAJES

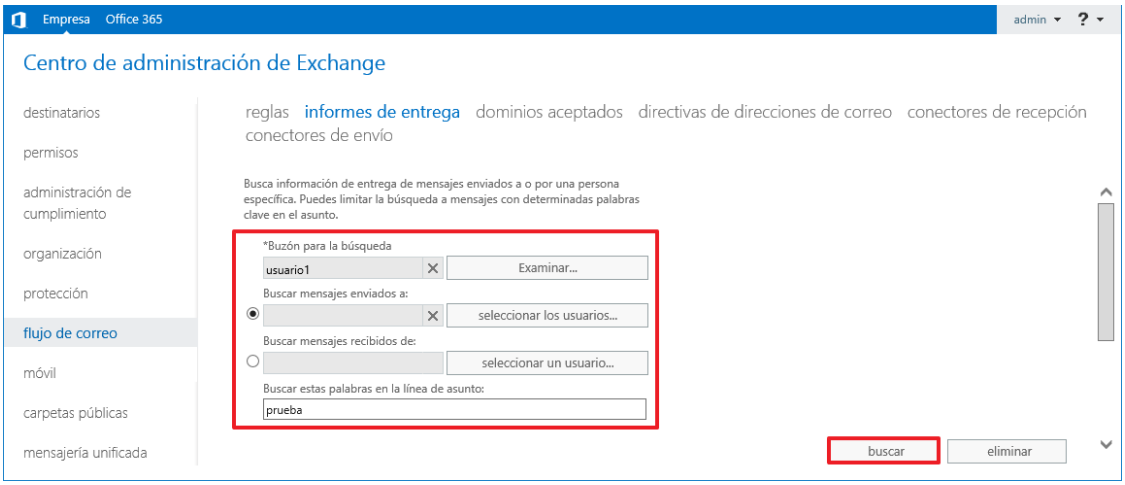
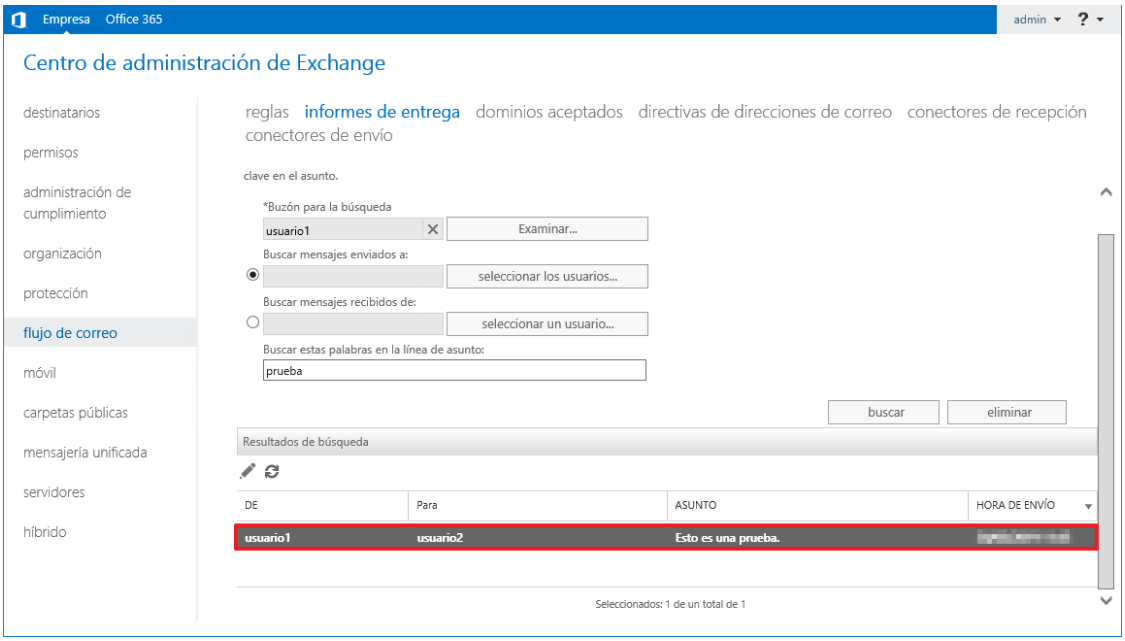
De forma predeterminada, Microsoft Exchange Server 2016 implementa mecanismos de registro para el seguimiento de mensajes y la conectividad de diferentes protocolos. Estos incluyen el envío y recepción de correos, así como la capacidad para analizar el estado de los mismos.

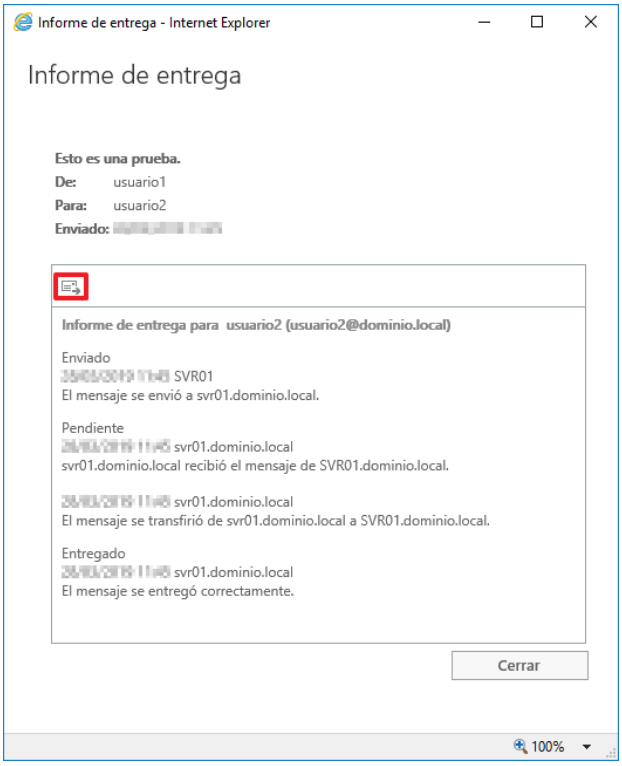
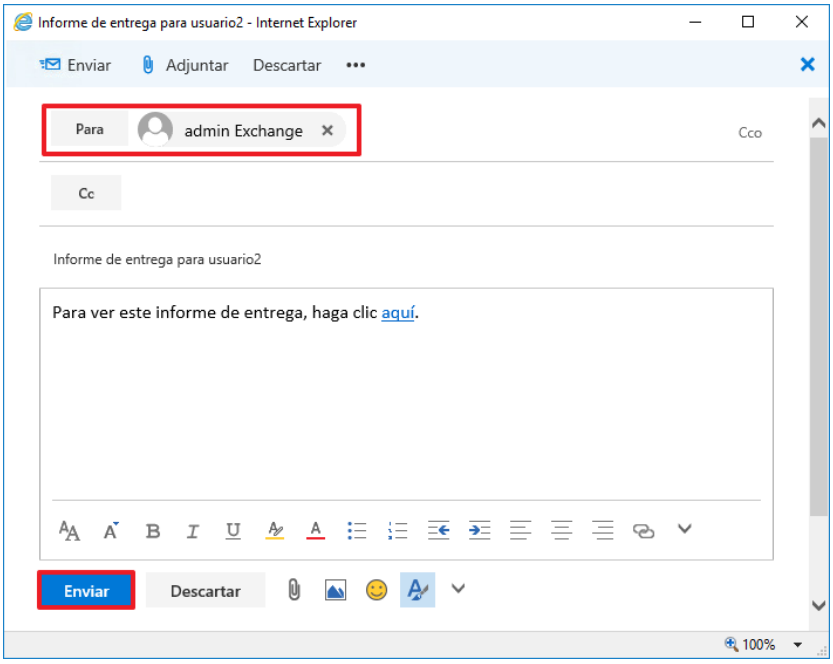
El seguimiento de mensajes se encuentra habilitado, así como los registros de protocolos de comunicaciones, pero podría necesitar modificarlos o bien si han sido desactivados en un momento determinado, poder habilitarlos nuevamente.

Paso	Descripción
118.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
119.	Pulse sobre "Internet Explorer" en la barra de tareas. 
120.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.

Paso	Descripción
121.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
122.	Dentro de la consola de administración de Exchange, seleccione el menú "servidores". A continuación, seleccione "servidores". 
123.	Seleccione el servidor con el rol "Buzón" y a continuación el botón de "Modificar" para dicho servidor. 

Paso	Descripción
124.	En la sección "Registros de transporte" puede modificar la configuración de almacenamiento de cada uno de los registros, así como habilitar y deshabilitar el "Registro de seguimiento de mensajes" y el "Registro de conectividad", tal y como se muestra a continuación. 
125.	Una vez modificadas las propiedades de acuerdo a las necesidades de su organización, pulse el botón "Guardar".
126.	El registro de seguimiento de seguimiento de mensajes lo puede ejecutar desde la propia consola Web de administración de Exchange Server 2016. Para ello, pulse sobre "flujo de correo" y posteriormente en "informes de entrega". 

Paso	Descripción
127.	Puede seleccionar el buzón en el que se desea buscar un mensaje, así como el remitente y/o el destinatario. Con la finalidad de reducir el número de resultados, se pueden escribir palabras clave en la línea de asunto (recuerde que esta funcionalidad sólo permite buscar por el asunto del mensaje y no su contenido).  **Nota:** En este ejemplo se ha utilizado el buzón "Usuario1" y la palabra clave "prueba".
128.	Los resultados se visualizarán en la zona inferior de la pantalla. Pulsando dos veces sobre cada uno de los resultados, se puede obtener un informe de seguimiento del mensaje. 

Paso	Descripción
129.	Así mismo, es posible que necesite enviar el informe de seguimiento al usuario afectado. Para ello pulse sobre el botón de envío y se generará un mensaje con un enlace para que el propio usuario lo pueda visualizar. 
130.	Especifique el destinatario y pulse sobre el botón "Enviar" para enviar el informe de entrega. 
131.	Una vez completadas las búsquedas de seguimiento de mensajes, pulse sobre el botón "Cerrar" y, a continuación, puede cerrar la sesión de la consola Web de administración de Exchange Server 2016.

3.10. PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD

Uno de los cambios más significativos desde Exchange 2013, es que RPC ya no es un protocolo de acceso directo compatible. Esto significa que la conectividad de Outlook en su totalidad debe realizarse a través del servidor de acceso de cliente mediante RPC sobre HTTP (también conocido como Outlook Anywhere).

El beneficio de este cambio es que no hay necesidad de tener el servicio de acceso de clientes de RPC en el servidor acceso de clientes. Esto ocasiona la reducción de dos espacios de nombres que habitualmente se necesitarían para una solución de resistencia ante fallos a nivel de sitios. Asimismo, ya no hay requerimientos para suministrar afinidad para el servicio de acceso de clientes de RPC.

Junto a esto, Exchange Server 2016 incorpora un protocolo de comunicación con los clientes Outlook denominado MAPI sobre HTTP (no confundir con RPC sobre HTTP o Outlook Anywhere).

MAPI sobre HTTP supone un avance importante en la simplificación de las comunicaciones de los clientes Outlook y el soporte de nuevos mecanismos de autenticación modernos como federación de identidades, autenticación de doble factor u otros.

MAPI sobre HTTP traslada la capa de transporte al modelo HTTP para mejorar la confiabilidad y la estabilidad de las conexiones de Outlook y Exchange. Esto permite un mayor nivel de visibilidad de los errores de transporte y una capacidad de recuperación mayor. Entre la funcionalidad adicional se incluye compatibilidad para una función de pausa y reanudación explícitas. Esto permite a los clientes compatibles cambiar de red o reactivarse después de la hibernación, manteniendo el mismo contexto de servidor.

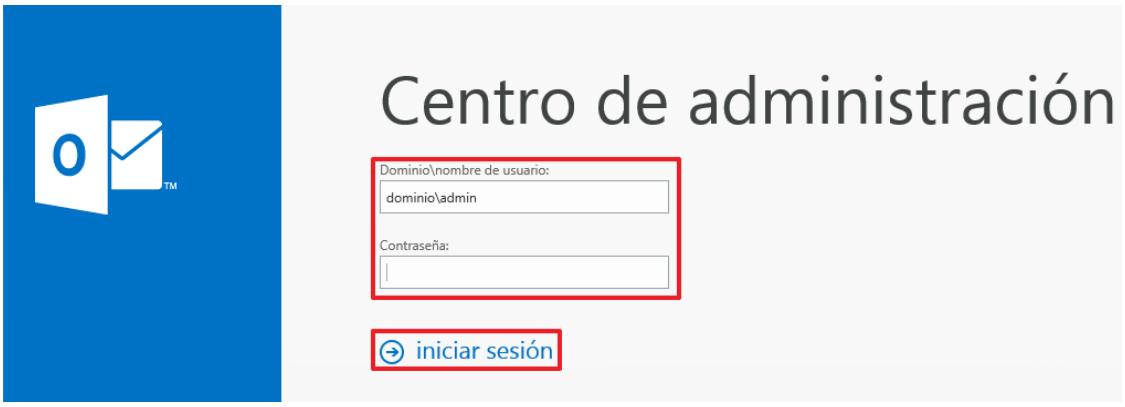
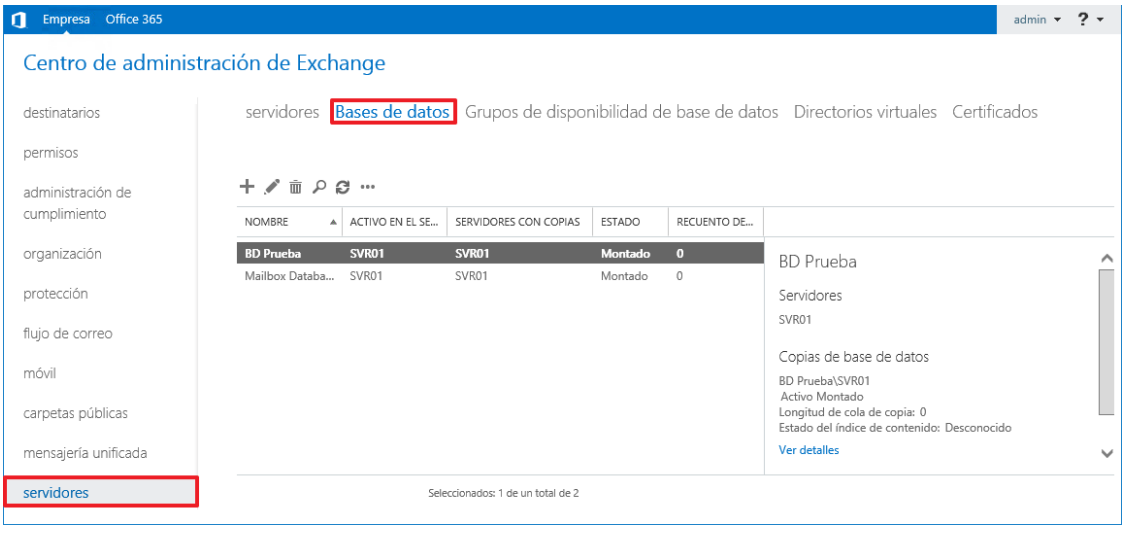
Microsoft Exchange Server 2016 incorpora estas características por defecto desde su instalación, por lo que, si no se desea degradar la seguridad es recomendable no deshabilitar el uso de estos protocolos.

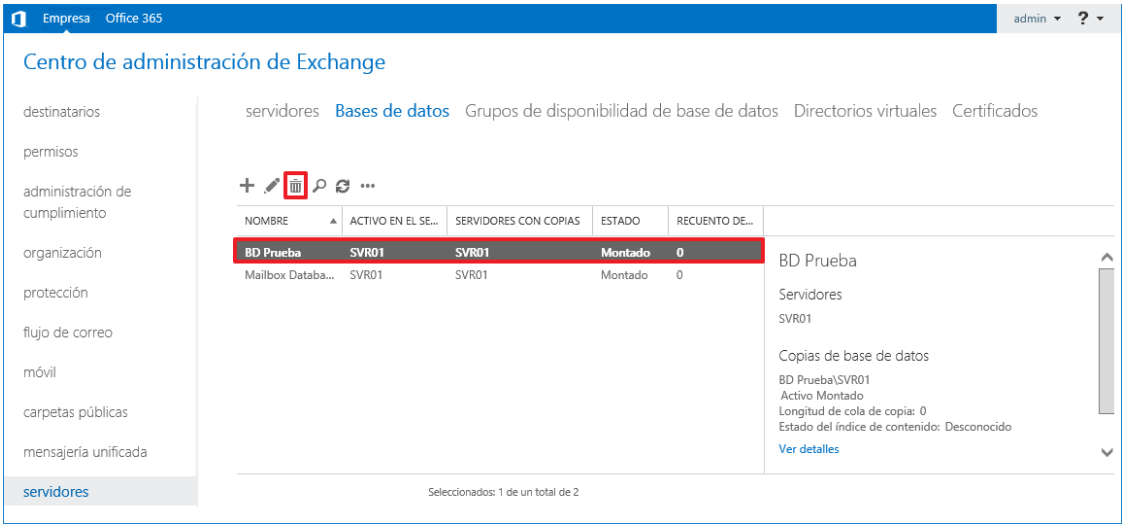
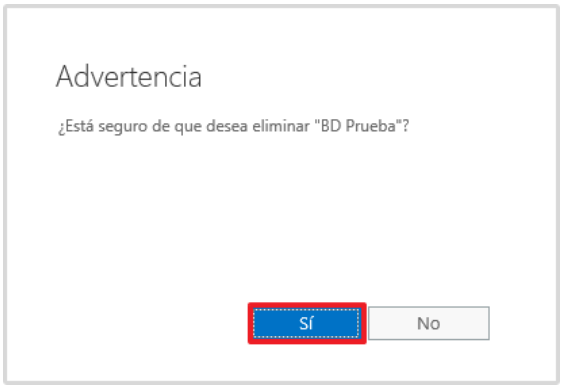
3.11. BORRADO SEGURO DE BASES DE DATOS

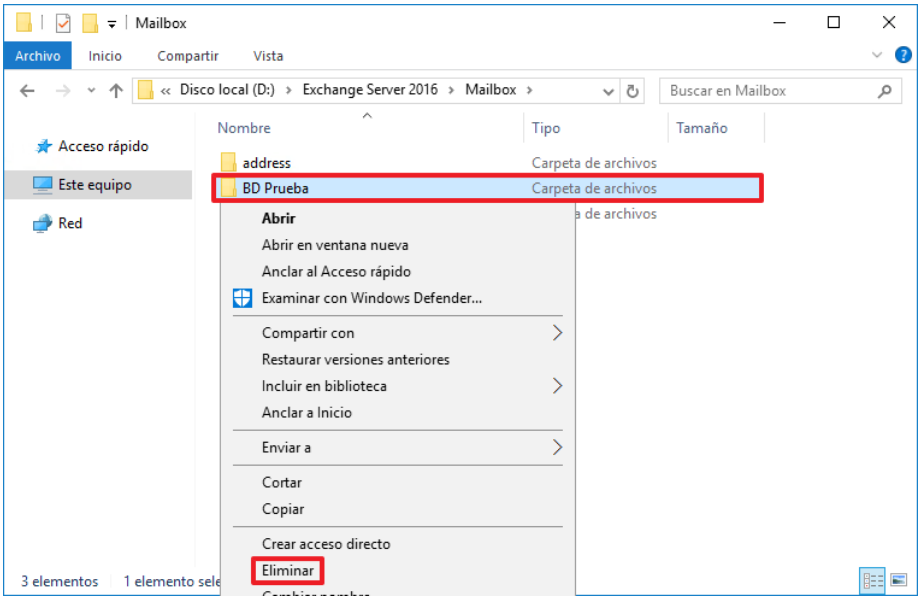
En Exchange Server 2016 edición Enterprise se pueden crear hasta 100 bases de datos por cada servidor de buzones, pudiendo alojar miles de buzones de usuarios en cada una de esas bases de datos. No existe un límite impuesto sobre el tamaño de las bases de datos y los buzones en Exchange Server 2016, aunque se recomienda que las bases de datos de buzones no superen los 200 GB para entornos no agrupados y de 2 TB para servidores de buzones en grupos de disponibilidad (DAG) con replicación habilitada.

A continuación, se detalla como eliminar una base de datos de buzones del servidor.

Paso	Descripción
132.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
133.	Pulse sobre "Internet Explorer" en la barra de tareas. 

Paso	Descripción
134.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.
135.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
136.	A continuación, diríjase a **"servidores → Bases de datos"**. 

Paso	Descripción
137.	Seleccione la base de datos que desea eliminar y pulse sobre "Borrar".  **Nota:** Si existen buzones alojados en la base de datos que desea eliminar debería previamente mover los buzones a otra base de datos para que el sistema permita eliminar la base de datos. En este ejemplo se elimina la base de datos "BD Prueba".
138.	Asegúrese que es correcta la base de datos que desea eliminar, y pulse "sí". 
139.	A continuación, le aparecerá una advertencia indicando que debe dirigirse a la ubicación física donde tenía alojada la base de datos y deberá eliminarla manualmente. Pulse "Aceptar" para cerrar la advertencia. 

Paso	Descripción
140.	Diríjase a la ubicación de la base de datos, seleccione la base de datos que acaba de eliminar de la consola de administración de Exchange 2016 y elimine manualmente la carpeta de la base de datos.  **Nota:** El sistema le solicitará elevación de privilegios para acceder a la ruta donde se alojan las bases de datos.

3.12. PROTECCIÓN DE DATOS Y RECUPERACIÓN DE ELEMENTOS ELIMINADOS

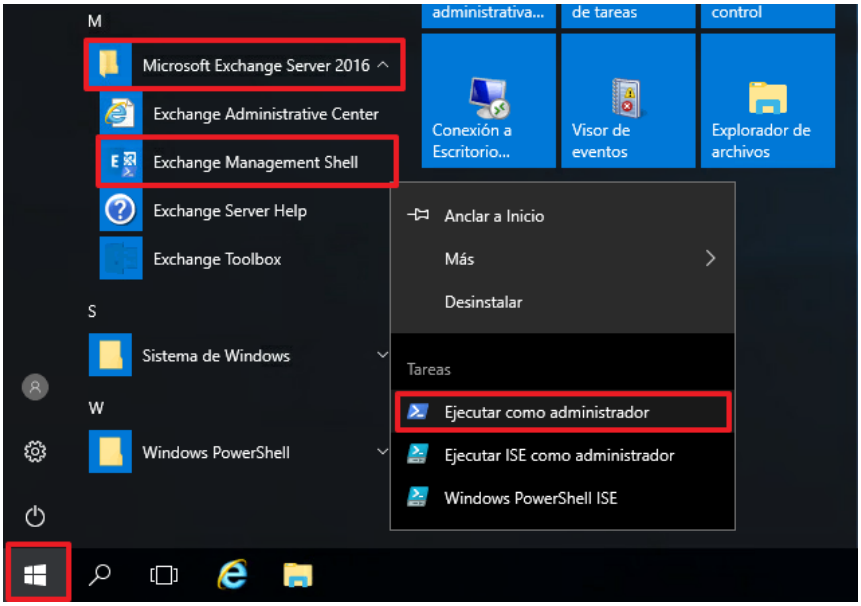
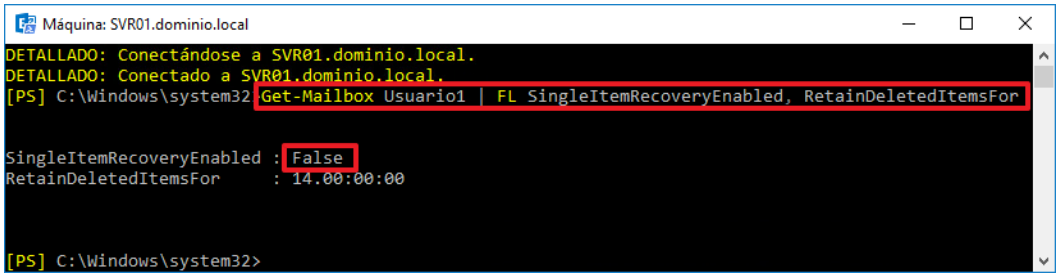
Microsoft para Exchange Server 2016 usa un concepto conocido como Exchange Native Data Protection, el cual se basa en características integradas de Exchange para proteger los datos de su buzón de correo sin tener que usar copias de seguridad (aunque puede seguir utilizando dichas características para crear copias de seguridad). Exchange 2016 incluye varias características nuevas y cambios generales que, una vez implementados y configurados correctamente, ofrecen una protección de datos nativa que elimina la necesidad de realizar copias de datos tradicionales.

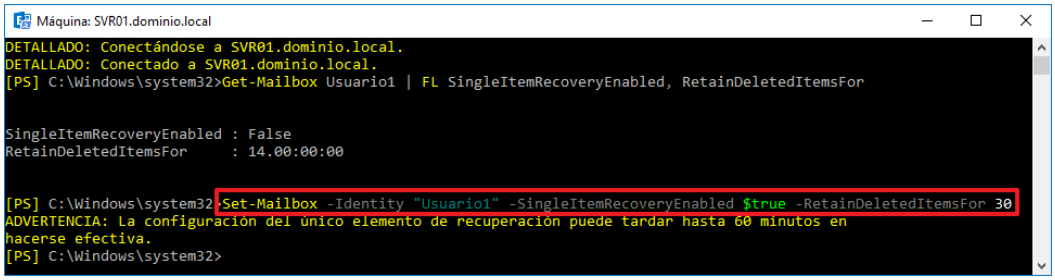
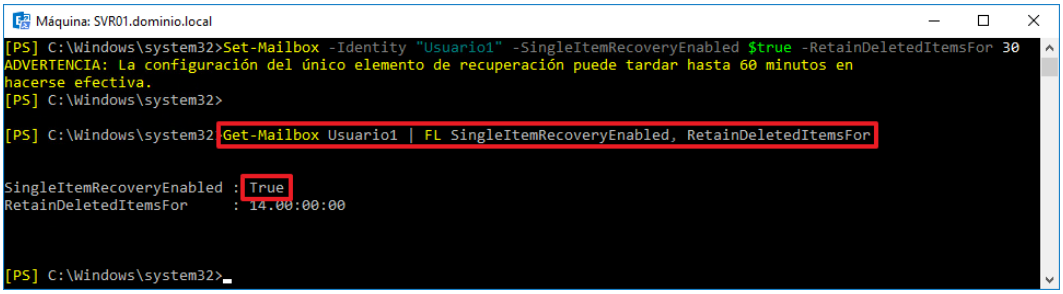
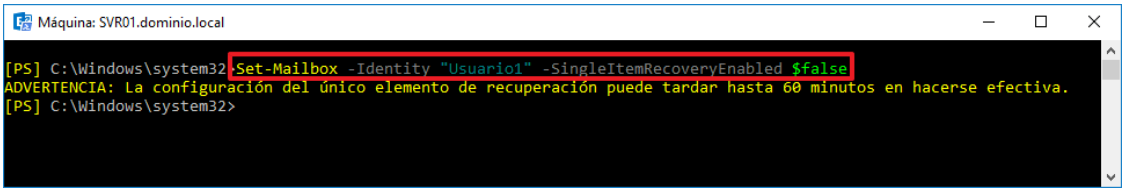
Exchange 2016 también implementa los grupos de disponibilidad de bases de datos (DAG). Un grupo de disponibilidad de base de datos (DAG) es el componente básico del marco de alta disponibilidad y resistencia de sitios del servidor de buzones que ofrece Microsoft Exchange Server 2016. Un DAG es un límite para la replicación de bases de datos de buzones, los cambios de bases de datos y de servidores, y las conmutaciones por error, así como para un componente interno denominado Active Manager.

Cualquier servidor en un DAG puede hospedar una copia de una base de datos de buzones de correo de cualquier otro servidor en el DAG. Cuando se agrega un servidor a un DAG funciona con los otros servidores del DAG para proporcionar recuperación automática de errores que afectan a las bases de datos de buzones, como un error de disco, de servidor o de red.

Además, Microsoft Exchange Server 2016, también ofrece la recuperación de un elemento único la cual se deshabilita cuando se crea un buzón. Si la recuperación de un elemento único está habilitada, los mensajes que el usuario elimina (purga) permanentemente se conservan en la carpeta "Elementos recuperables" del buzón hasta que expira el período de retención de elementos eliminados. Esto permite al administrador recuperar los mensajes purgados por el usuario antes de que expire el período de retención de elementos eliminados.

A continuación, se muestra como habilitar la recuperación de un elemento único el cual viene deshabilitado por defecto.

Paso	Descripción
141.	Inicie sesión en el servidor miembro donde está instalado Microsoft Exchange Server 2016 con un usuario con permisos de administrador.
142.	Pulse sobre el menú inicio despliegue la carpeta "Microsoft Exchange Server 2016" y pulsando con botón derecho en "Exchange Management Shell" seleccione "Ejecutar como administrador".  **Nota:** El sistema le solicitará elevación de privilegios.
143.	A continuación, si desea comprobar si está habilitada la recuperación ejecute el comando y compruebe que el estado es "False". – "Get-Mailbox <Nombre_buzon> | FL SingleItemRecoveryEnabled, RetainDeletedItemsFor" Sustituya "<Nombre_buzon>" por el nombre de buzón que desea comprobar. 

Paso	Descripción
144.	A continuación, para habilitar la recuperación de elementos eliminados ejecute el siguiente comando. – "Set-Mailbox -Identity "Usuario1" -SingleItemRecoveryEnabled $true -RetainDeletedItemsFor 30" Además, se establecerá que el tiempo de conservación de los correos será de 30 días. 
145.	Compruebe que ha habilitado correctamente la recuperación de elementos eliminados. Ejecute nuevamente el siguiente comando. – "Get-Mailbox <Nombre_buzon> | FL SingleItemRecoveryEnabled, RetainDeletedItemsFor" Compruebe que el estado es "True". 
146.	En caso de que desee deshabilitar la recuperación de elementos eliminados deberá ejecutar el comando. – "Set-Mailbox -Identity "Nombre_Usuario" -SingleItemRecoveryEnabled $false"  **Nota:** Si desea más información acerca de la recuperación de elementos eliminados en Exchange Server 2016 visite el sitio web: https://technet.microsoft.com/es-es/library/ee633460(v=exchg.150).aspx

3.13. PROTECCIÓN DE SERVICIOS

Exchange Server 2016 utiliza IIS por lo que todos los sistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que le competen como:

a) Ataques directos, tales como accesos no autorizados sobre cualquiera de los elementos que conforman el entorno.

b) Ataques indirectos, dónde cualquiera de los elementos es empleado como herramienta en el ataque.

c) Ataques de denegación de servicio (DoS). Las arquitecturas Web están basadas en tecnologías TCP/IP y por tanto son vulnerables a los ataques de DoS comunes en TCP/IP. Es necesario disponer de contramedidas técnicas y procedimientos de actuación frente a este tipo de ataques.

Para una mayor seguridad sobre Exchange Server 2016 se han de configurar los filtros de solicitudes los cuales permiten controlar las conexiones entre servidor y cliente, restringiendo el comportamiento de protocolos y contenidos.

Se considera una buena práctica de seguridad realizar una configuración básica para el servidor según los usos, situación, contenidos a servir, etc. que se le prevén y luego afinar aún más en cada uno de los sitios que se generen.

El filtro de solicitudes es un módulo, o servicio de rol, de IIS instalable (por medio de AppCMD.exe, Administrador del servidor, Powershell, etc.) de forma individual y configurable por cualquiera de los medios habituales (Administrador de Internet Information Services (IIS), AppCMD.exe, etc.).

En el apartado "2 PREPARACIÓN DEL IIS 10" se aplica seguridad sobre URLfiltering para Microsoft Exchange Server 2016.

ANEXO A.2.2. LISTA DE COMPROBACIÓN

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

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

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

1. COMPROBACIONES EN CONTROLADOR DE DOMINIO

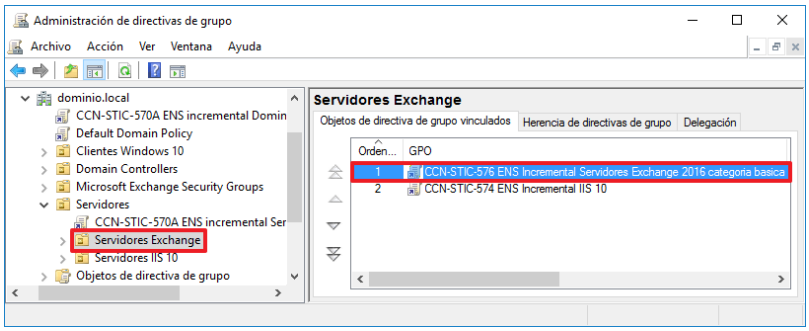
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador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

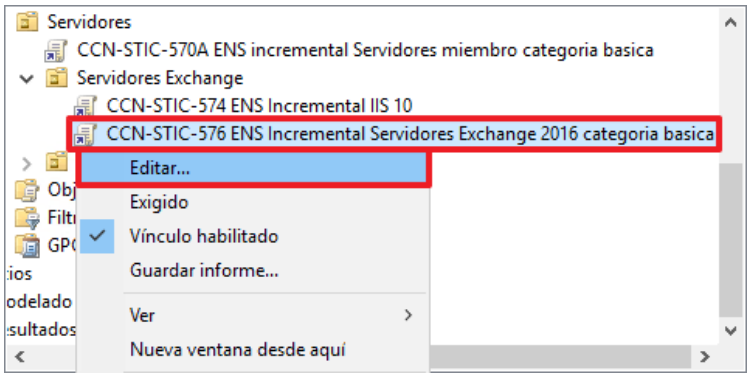
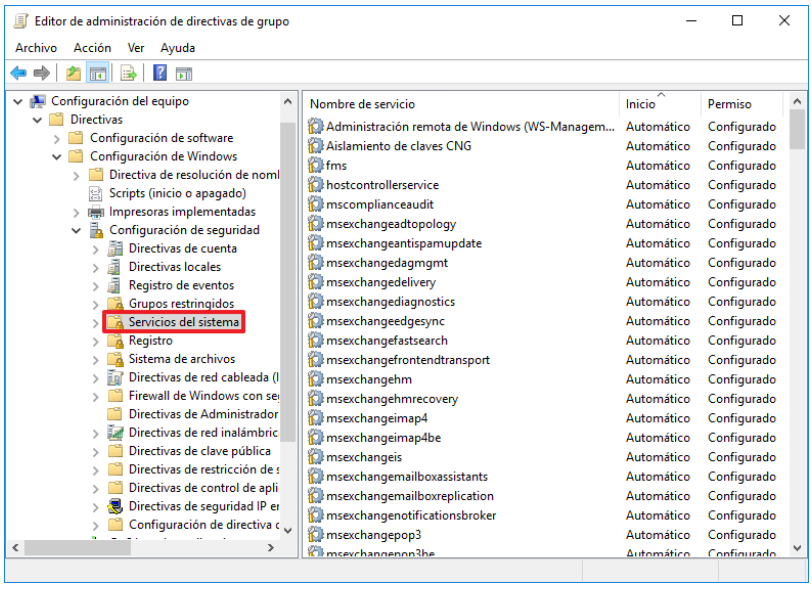
a) Usuarios y equipos de Active Directory (dsa.msc).

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

c) Editor de objetos de directiva de grupo (gpedit.msc).

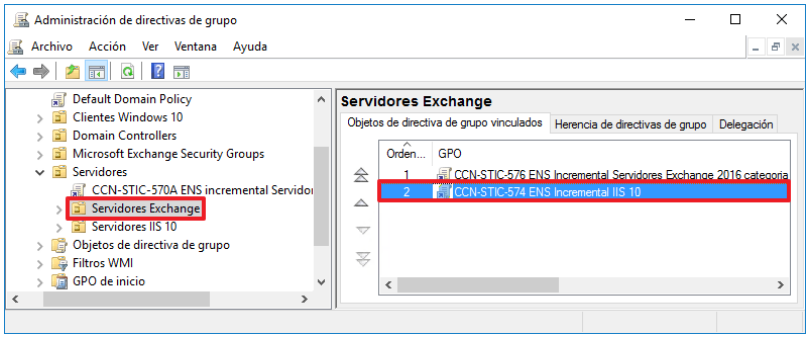
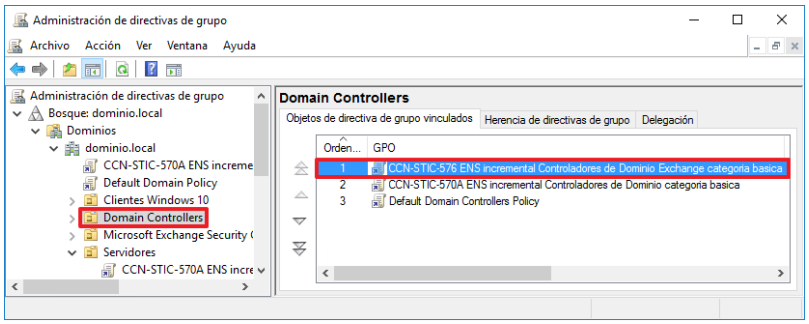
Nota: La lista de comprobación está basada en los nombres de objetos de directivas, unidades organizativas y cuentas de servicios tal y como se ha indicado durante la presente guía. Deberá adaptar los pasos según la configuración de su organización.

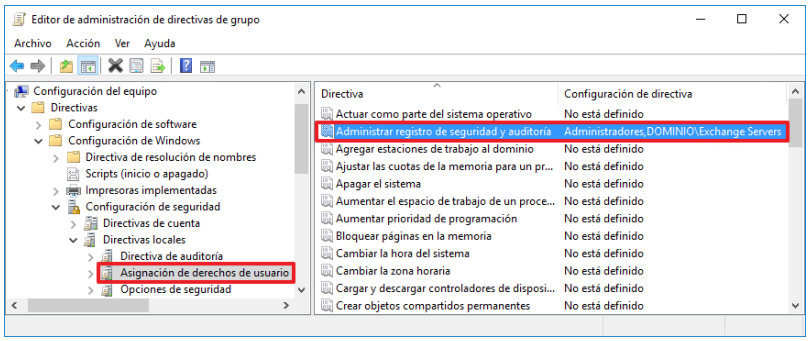
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
2. Verifique que está creada la directiva de Exchange 2016 (CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria basica).		Ejecute la herramienta "Administración de directivas de grupo" desde "**Administrador del servidor → Herramientas → Administración de directivas de grupo**". El sistema le solicitará elevación de privilegios para acceder al administrador del servidor. Seleccione la unidad organizativa "Servidores Exchange", situada en **"Bosque → Dominios → [Su_dominio] → Servidores → Servidores Exchange"** y a continuación, en el panel de la derecha, verifique que está creado el objeto de directiva de grupo denominado "CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria basica" y se encuentra en el primer orden de directivas de grupo vinculados. 

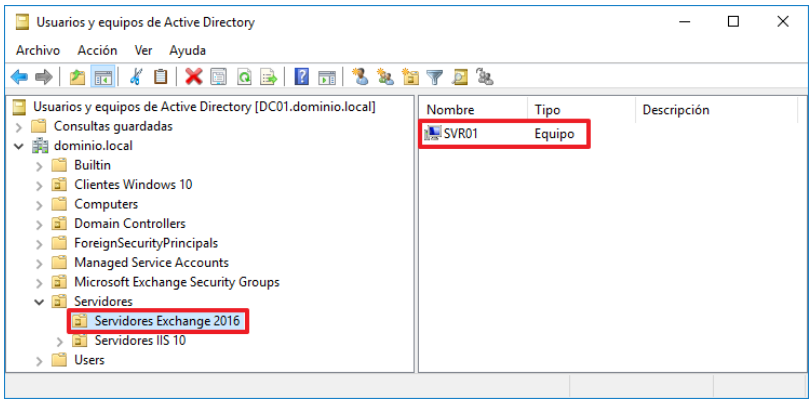
Comprobación	OK/NOK	Cómo hacerlo
		Seleccione con el botón derecho el objeto de directiva de grupo y haga clic en la opción "Editar" del menú para verificar los valores de la directiva "CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria basica". 
3. Verifique los valores de los servicios del sistema de la directiva CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria basica.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria básica" tiene los siguientes valores de servicios de sistema. **"Directiva CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema".**  **Nota:** Puede ordenar los servicios por la columna "Inicio". Dependiendo de los servicios que estén instalados en el controlador de dominio utilizado para la verificación, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales. Cuando finalice, cierre el editor de objetos de directiva de grupo.

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permisos**	**OK/NOK**	
Actualización de correo no deseado de Microsoft Exchange	msexchangeantispamupdate	Automático	Configurado		
Administración de Microsoft Exchange DAG	msexchangedagmgmt	Automático	Configurado		
Administración remota de Windows (WS-Management)	Winrm	Automático	Configurado		
Administrador del estado de Microsoft Exchange	msexchangehm	Automático	Configurado		
Aislamiento de claves CNG	keyiso	Automático	Configurado		
Asistentes de buzón de Microsoft Exchange	msexchangemailboxassistants	Automático	Configurado		
ASP.NET State Service	aspnet_state	Manual	Configurado		
Host de servicios de cumplimiento de normas.	msexchangecompliance	Automático	Configurado		
Auditoría de conformidad de Microsoft Exchange	mscomplianceaudit	Automático	Configurado		
Back- end POP3 de Microsoft de Microsoft Exchange	msexchangepop3be	Deshabilitado	Configurado		
Back-end IMAP 4 de Microsoft Exchange	msexchangeimap4be	Deshabilitado	Configurado		
Búsqueda de Microsoft Exchange	msexchangefastsearch	Automático	Configurado		
Diagnósticos de Microsoft Exchange	msexchangediagnostics	Automático	Configurado		
Enrutador de llamadas de mensajería unificada de Microsoft Exchange	msexchangeumcr	Automático	Configurado		
Entrega de transporte de buzones de Microsoft Exchange	msexchangedelivery	Automático	Configurado		
Envío de transporte de buzones de Microsoft Exchange	msexchangesubmission	Automático	Configurado		
Límite de Microsoft Exchange	msexchangethrottling	Automático	Configurado		
Mensajería unificada de Microsoft Exchange	msexchangeum	Automático	Configurado		
Microsoft Exchange EdgeSync	msexchangeedgesync	Automático	Configurado		
Microsoft Exchange IMAP4	msexchangeimap4	Deshabilitado	Configurado		
Microsoft Exchange Information Store	msexchangeis	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permisos**	**OK/NOK**	
Microsoft Exchange Notifications Broker	msexchangenotificationsbroker	Automático	Configurado		
Microsoft Exchange POP3	msexchangepop3	Deshabilitado	Configurado		
Microsoft Exchange Search Host Controller	hostcontrollerservice	Automático	Configurado		
Microsoft Exchange Server Extension for Windows Server Backup	wsbexchange	Manual	Configurado		
Microsoft Exchange Service Host	msexchangeservicehost	Automático	Configurado		
Notificaciones del servicio de token de Windows	c2wts	Manual	Configurado		
Recuperación del administrador del estado de Microsoft Exchange	msexchangehmrecovery	Automático	Configurado		
Registro de búsquedas de Transport de Microsoft Exchange	msexchangetransportlogsearch	Automático	Configurado		
Registro remoto	remoteregistry	Automático	Configurado		
Replicación de buzón de Microsoft Exchange	msexchangemailboxreplication	Automático	Configurado		
Replicación de Microsoft Exchange	msexchangerepl	Automático	Configurado		
Servicio de acceso de cliente RPC de Microsoft Exchange	msexchangerpc	Automático	Configurado		
Servicio de administración de filtrado de Microsoft	fms	Automático	Configurado		
Servicio de equilibrio de carga RPC/HTTP	rpchttplbs	Manual	Configurado		
Servicio de uso compartido de puertos Net.Tcp	nettcpportsharing	Automático	Configurado		
Servicio WAS (Windows Process Activation Service)	was	Automático	Configurado		
Servidor	lanmanserver	Automático	Configurado		
Sistema de eventos COM+	eventsystem	Manual	Configurado		
Topología de Active Directory de Microsoft Exchange	msexchangeadtopology	Automático	Configurado		
Tracing Service for Search in Exchange	searchexchangetracing	Automático	Configurado		
Transport de Microsoft Exchange	msexchangetransport	Automático	Configurado		
Transporte Frontend de Microsoft Exchange	msexchangefrontendtransport	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo
4. Verifique que está creada la directiva de Internet Information Services 10 (CCN-STIC-574 ENS Incremental IIS 10).		Sin salir de la consola "Administración de directivas de grupo", seleccione la unidad organizativa "Servidores Exchange", situada en **"Bosque → Dominios → [Su_dominio] → Servidores → Servidores Exchange"** y a continuación, verifique que está creado el objeto de directiva de grupo denominado "CCN-STIC-574 ENS Incremental IIS 10".  **Nota:** La configuración de seguridad de esta GPO deberá de haberse comprobado en la guía codificada como "CCN-STIC-574".
5. Verifique que está creada la directiva CCN-STIC-576 ENS Incremental Controladores de Dominio Exchange categoria basica.		Sin salir de la consola "Administración de directivas de grupo", seleccione la unidad organizativa "Servidores Exchange", situada en **"Bosque → Dominios → [Su_dominio] → Domain Controllers"** y a continuación, verifique que está creado el objeto de directiva de grupo denominado "CCN-STIC-576 ENS Incremental Controladores de Dominio Exchange categoria basica" y se encuentra en el primer orden de vínculos. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>6. Verifique los valores de seguridad de la directiva CCN-STIC-576 ENS Incremental Controladores de Dominio Exchange categoria basica.</td><td></td><td>Utilizando el editor de objetos de directiva de grupo, verifique que la directiva CCN-STIC-576 Incremental Controlador de Dominio Exchange tiene el siguiente valor de seguridad.
“CCN-STIC-576 ENS Incremental Controladores de Dominio Exchange categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Administrar registro de seguridad y auditoría</td><td>Administradores Exchange Servers</td><td></td></tr>
</table></td></tr>
<tr><td>7. Verifique que los servidores a asegurar están dentro de la unidad organizativa “Servidores Exchange”.</td><td></td><td>Ejecute la herramienta “Usuarios y equipos de Active Directory” desde “Administrador del servidor → Herramientas → Usuarios y equipos de Active Directory”. El sistema le solicitará elevación de privilegios para acceder al administrador del servidor.
A continuación, seleccione la unidad organizativa “Servidores Exchange” y verifique que se encuentra el servidor donde se ha instalado Exchange Server 2016.
 
</td></tr>
</table>

2. COMPROBACIONES EN SERVIDOR MIEMBRO

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:

a) Administrador de Windows (explorer.exe).

b) Símbolo del sistema (cmd.exe).

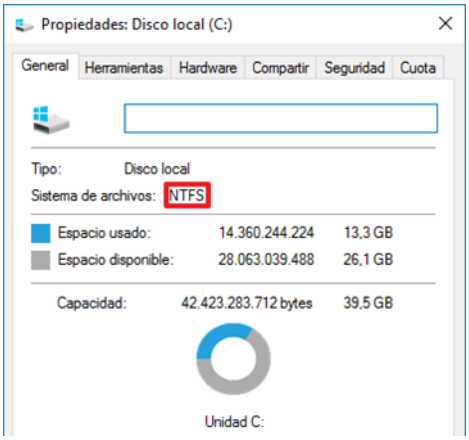
c) Servicios (services.msc).

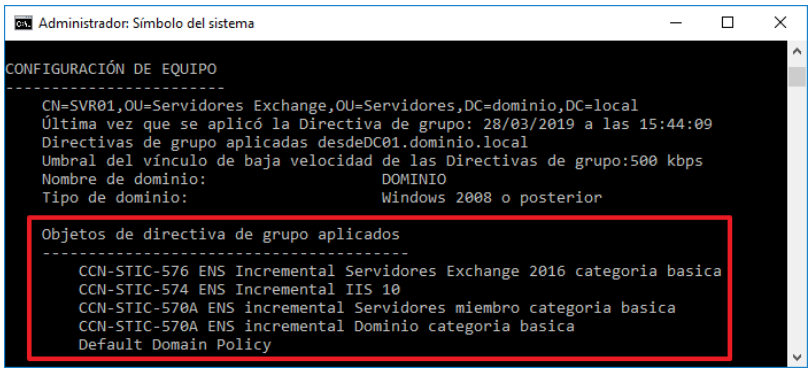
d) Editor de objetos de directiva de grupo (gpedit.msc).

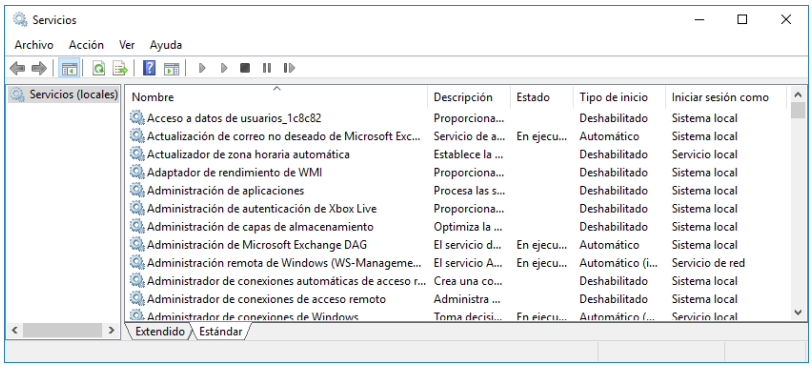
e) Administrador de Internet Information Services (iis.msc).

f) Consola Web de administración de Exchange 2016.

g) Shell de administración de Exchange 2016.

Comprobación	OK/NOK	Cómo hacerlo
8. Inicie sesión en los servidores Exchange 2016.		A continuación, para completar el resto de la lista de comprobación deberá iniciar sesión en el servidor donde se aloja Exchange Server 2016 con una cuenta que tenga permisos de administrador local del servidor, administrador del dominio o administrador de la organización de Exchange.
9. Verifique que todos los volúmenes están formateados con NTFS.		Utilizando el explorador de Windows (botón derecho sobre **Inicio → Explorador de archivos, botón derecho sobre la unidad C:\ → Propiedades**), verifique en las propiedades de cada partición el uso del sistema de archivos NTFS o cualquier sistema de archivos que permita ACL's. 

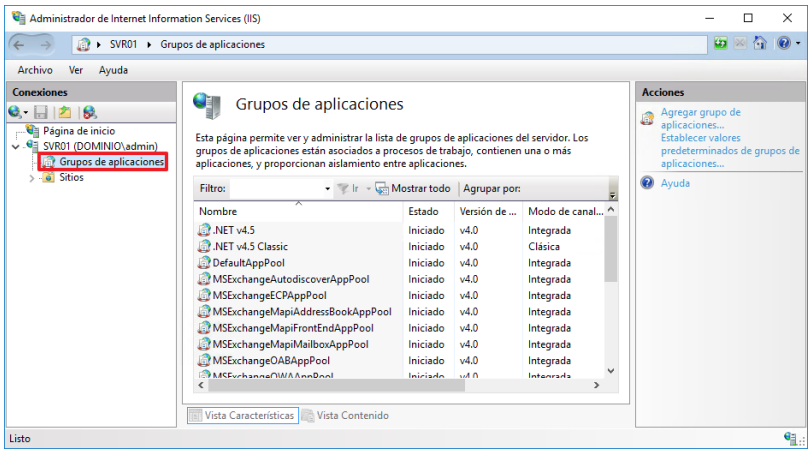
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>10. Verifique que le están aplicando las GPO de forma correcta.</td><td></td><td>Abra una consola de comandos como administrador con botón derecho en “Inicio → Símbolo del sistema (administrador)” y ejecute el comando “gpresult –r”. Compruebe que las GPO están aplicando al equipo en el orden correcto.
 

<table>
<tr><th>Objeto de directiva de grupo</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria basica</td><td></td></tr>
<tr><td>CCN-STIC-574 ENS Incremental IIS 10</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS incremental Servidores miembro categoria basica</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS Incremental Dominio categoria basica</td><td></td></tr>
<tr><td>Default Domain Policy</td><td></td></tr>
</table></td></tr>
<tr><td>11. Verifique que los servicios del sistema están configurados de forma correcta.</td><td></td><td>Ejecute la herramienta “Servicios” desde “Administrador del servidor → Herramientas → Servicios”. El sistema le solicitará elevación de privilegios para acceder al administrador del servidor.
 

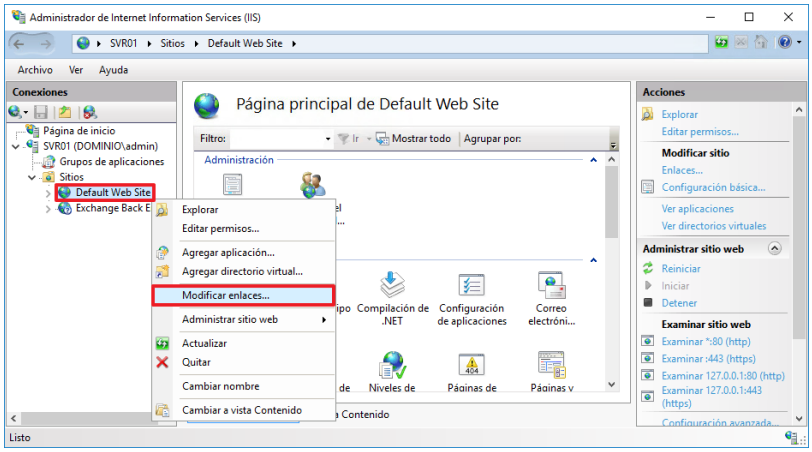
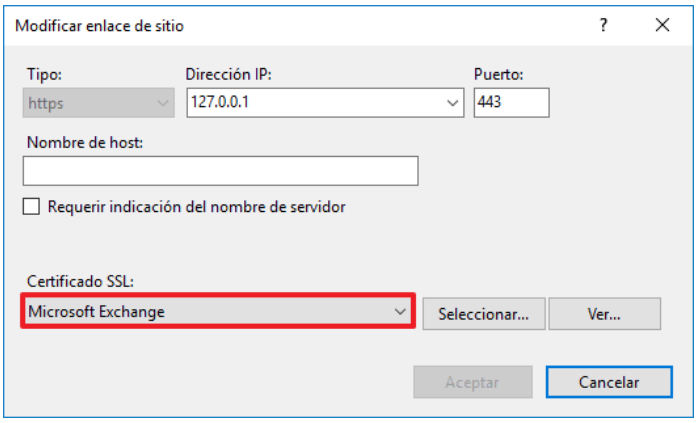
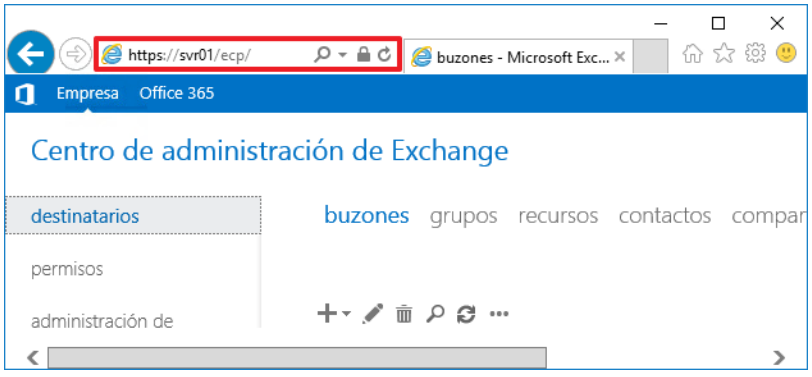
Nota: Dependiendo del equipo, es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales. Puede ordenar los servicios por “Tipo de inicio”. Sólo se verifican los servicios que configura esta guía.</td></tr>
</table>

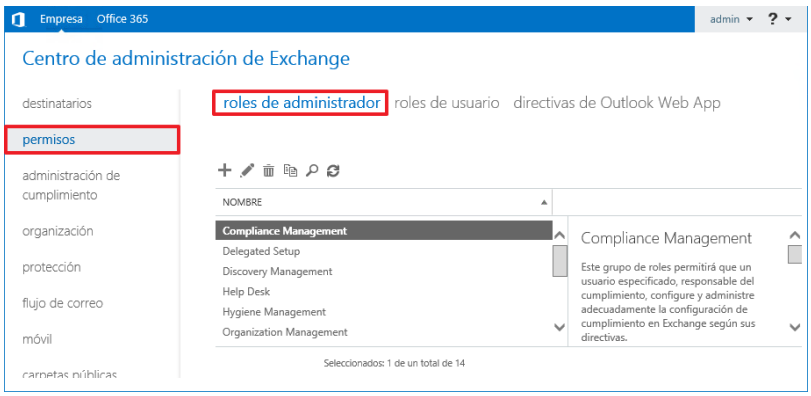
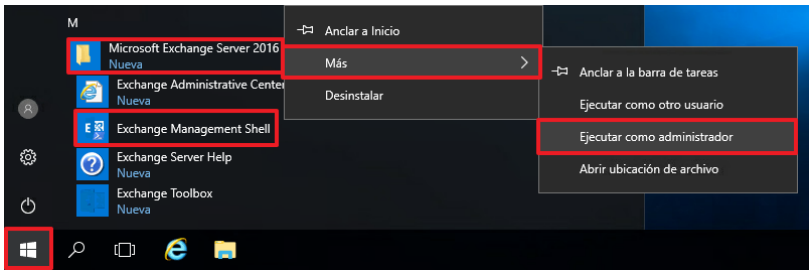
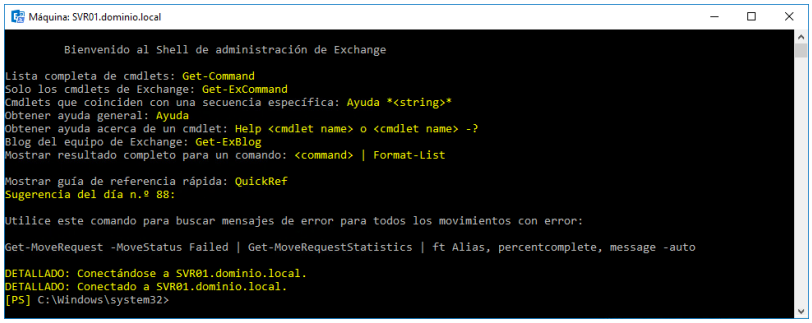
Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permisos**	**OK/NOK**	
Actualización de correo no deseado de Microsoft Exchange	msexchangeantispamupdate	Automático	Configurado		
Administración de Microsoft Exchange DAG	msexchangedagmgmt	Automático	Configurado		
Administración remota de Windows (WS-Management)	winrm	Automático	Configurado		
Administrador del estado de Microsoft Exchange	msexchangehm	Automático	Configurado		
Aislamiento de claves CNG	keyiso	Automático	Configurado		
Asistentes de buzón de Microsoft Exchange	msexchangemailboxassistants	Automático	Configurado		
ASP.NET State Service	aspnet_state	Manual	Configurado		
Auditoría de conformidad de Microsoft Exchange	mscomplianceaudit	Automático	Configurado		
Servicio de cumplimiento de normas de Microsoft Exchange.	msexchangecompliance	Automático	Configurado		
Back- end POP3 de Microsoft de Microsoft Exchange	msexchangepop3be	Deshabilitado	Configurado		
Back-end IMAP 4 de Microsoft Exchange	msexchangeimap4be	Deshabilitado	Configurado		
Búsqueda de Microsoft Exchange	msexchangefastsearch	Automático	Configurado		
Diagnósticos de Microsoft Exchange	msexchangediagnostics	Automático	Configurado		
Enrutador de llamadas de mensajería unificada de Microsoft Exchange	msexchangeumcr	Automático	Configurado		
Entrega de transporte de buzones de Microsoft Exchange	msexchangedelivery	Automático	Configurado		
Envío de transporte de buzones de Microsoft Exchange	msexchangesubmission	Automático	Configurado		
Límite de Microsoft Exchange	msexchangethrottling	Automático	Configurado		
Mensajería unificada de Microsoft Exchange	msexchangeum	Automático	Configurado		
Microsoft Exchange EdgeSync	msexchangeedgesync	Automático	Configurado		
Microsoft Exchange IMAP4	msexchangeimap4	Deshabilitado	Configurado		
Microsoft Exchange Information Store	msexchangeis	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permisos**	**OK/NOK**	
Microsoft Exchange Notifications Broker	msexchangenotificationsbroker	Automático	Configurado		
Microsoft Exchange POP3	msexchangepop3	Deshabilitado	Configurado		
Microsoft Exchange Search Host Controller	hostcontrollerservice	Automático	Configurado		
Microsoft Exchange Server Extension for Windows Server Backup	wsbexchange	Manual	Configurado		
Microsoft Exchange Service Host	msexchangeservicehost	Automático	Configurado		
Notificaciones del servicio de token de Windows	c2wts	Manual	Configurado		
Recuperación del administrador del estado de Microsoft Exchange	msexchangehmrecovery	Automático	Configurado		
Registro de búsquedas de Transport de Microsoft Exchange	msexchangetransportlogsearch	Automático	Configurado		
Registro remoto	remoteregistry	Automático	Configurado		
Replicación de buzón de Microsoft Exchange	msexchangemailboxreplication	Automático	Configurado		
Replicación de Microsoft Exchange	msexchangerepl	Automático	Configurado		
Servicio de acceso de cliente RPC de Microsoft Exchange	msexchangerpc	Automático	Configurado		
Servicio de administración de filtrado de Microsoft	fms	Automático	Configurado		
Servicio de equilibrio de carga RPC/HTTP	rpchttplbs	Manual	Configurado		
Servicio de uso compartido de puertos Net.Tcp	nettcpportsharing	Automático	Configurado		
Servicio WAS (Windows Process Activation Service)	was	Automático	Configurado		
Servidor	lanmanserver	Automático	Configurado		
Sistema de eventos COM+	eventsystem	Manual	Configurado		
Topología de Active Directory de Microsoft Exchange	msexchangeadtopology	Automático	Configurado		
Tracing Service for Search in Exchange	searchexchangetracing	Automático	Configurado		
Transport de Microsoft Exchange	msexchangetransport	Automático	Configurado		
Transporte Frontend de Microsoft Exchange	msexchangefrontendtransport	Automático	Configurado		

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>12. En el servidor Exchange, verifique que se han creado los grupos de aplicaciones correspondientes.</td><td></td><td>Ejecute la herramienta “Administrador de Internet Information Services (IIS)” desde “Administrador del servidor → Herramientas → Administrador de Internet Information Services (IIS)”. El sistema le solicitará elevación de privilegios para acceder al administrador del servidor.
Seleccione el nodo “Nombre_Servidor → Grupo de aplicaciones” y verifique que existen los siguientes grupos de aplicaciones de Exchange.
 

<table>
<tr><th>Grupos de aplicaciones</th><th>OK/NOK</th></tr>
<tr><td>.Net v4.5</td><td></td></tr>
<tr><td>.Net v4.5 Classic</td><td></td></tr>
<tr><td>DefaultAppPool</td><td></td></tr>
<tr><td>MSExchangeAutodiscoverAppPool</td><td></td></tr>
<tr><td>MSExchangeECPAppPool</td><td></td></tr>
<tr><td>MSExchangeMAPIAddressBookAppPool</td><td></td></tr>
<tr><td>MSExchangeMAPIFrontEndAppPool</td><td></td></tr>
<tr><td>MSExchangeMAPIMailboxAppPool</td><td></td></tr>
<tr><td>MSExchangeOABAppPool</td><td></td></tr>
<tr><td>MSExchangeOWAAppPool</td><td></td></tr>
<tr><td>MSExchangeOWACalendarAppPool</td><td></td></tr>
<tr><td>MSExchangePowerShellAppPool</td><td></td></tr>
<tr><td>MSExchangePowerShellFrontEndAppPool</td><td></td></tr>
<tr><td>MSExchangePushNotificationsAppPool</td><td></td></tr>
<tr><td>MSExchangeRestAppPool</td><td></td></tr>
<tr><td>MSExchangeRestFrontEndAppPool</td><td></td></tr>
<tr><td>MSExchangeRPCProxyAppPool</td><td></td></tr>
<tr><td>MSExchangeRPCProxyFrontEndAppPool</td><td></td></tr>
<tr><td>MSExchangeServicesAppPool</td><td></td></tr>
<tr><td>MSExchangeSyncAppPool</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
13. En el servidor Exchange, verifique que se ha establecido el certificado correspondientes.		En la herramienta "Administrador de Internet Information Services (IIS)" seleccione con botón derecho el nodo **"Nombre_Servidor → Sitios → Default Web Site"** y pulse sobre "Modificar enlaces…".  Confirme que está seleccionado el certificado SSL correcto en el enlace de tipo https con puerto 443. 
14. Verifique el acceso la consola Web de Exchange Server 2016 se realiza de forma correcta.		Inicie sesión en la consola de administración de Exchange desde el navegador.  **Nota:** En este ejemplo se usa https://SVR01/ecp.

Comprobación	OK/NOK	Cómo hacerlo
15. Confirme que se ha creado un grupo de auditoría.		Pulse en **"Permisos → roles de administrador"** y confirme que se han aplicado los permisos adecuados a su organización. 
16. En el servidor Exchange, verifique el acceso correcto al Shell de Exchange Server 2016.		Inicie sesión en el Shell de administración de Exchange desde el menú **"Inicio → Todas las aplicaciones → Microsoft Exchange Server 2016"** y pulse con botón derecho en "Exchange Management Shell". El sistema le solicitará elevación de privilegios.  Tras introducir las credenciales, compruebe que se ejecute "Exchange Management Shell" correctamente como aparece en la siguiente imagen. 

ANEXO A.3. CATEGORÍA MEDIA

ANEXO A.3.1. PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE EXCHANGE SERVER 2016 SOBRE MICROSOFT 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 emplee el producto Microsoft Exchange Server 2016 sobre Windows Server 2016, con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad.

Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar la categoría de cada una de las dimensiones de seguridad, según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización 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, se deberán realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

Microsoft Exchange Server 2016 requiere de otros servicios adicionales para su instalación y correcto funcionamiento, por lo que es necesario realizar una preparación previa del entorno antes de instalar Microsoft Exchange Server 2016.

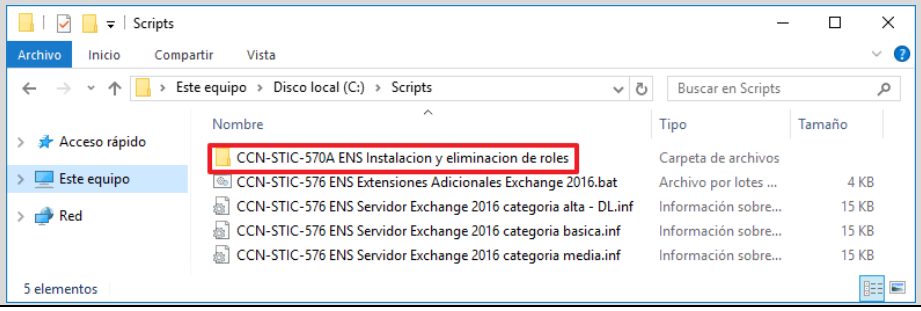
En caso de necesitar información sobre los requisitos previos de instalación de Microsoft Exchange Server 2016, visite el siguiente enlace: https://docs.microsoft.com/es-es/Exchange/plan-and-deploy/prerequisites?view=exchserver -2016

Antes de iniciar las operaciones de implementación es necesario disponer de los siguientes elementos:

a) Un servidor controlador de dominio Windows Server 2016 que haya sido preparado siguiendo la guía de seguridad CCN-STIC-570A Anexo A con una categorización de seguridad media.

b) Un servidor miembro del dominio con el servicio Web Internet Information Services instalado y preparado siguiendo las guías CCN-STIC-570A Anexo A y CCN-STIC-574 Anexo A con una categorización de seguridad media.

Nota: Si instala Exchange 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.

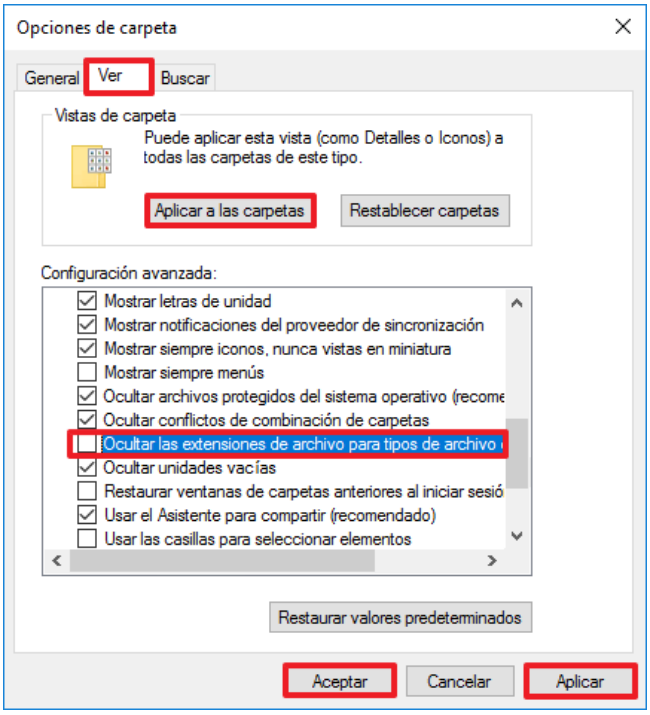


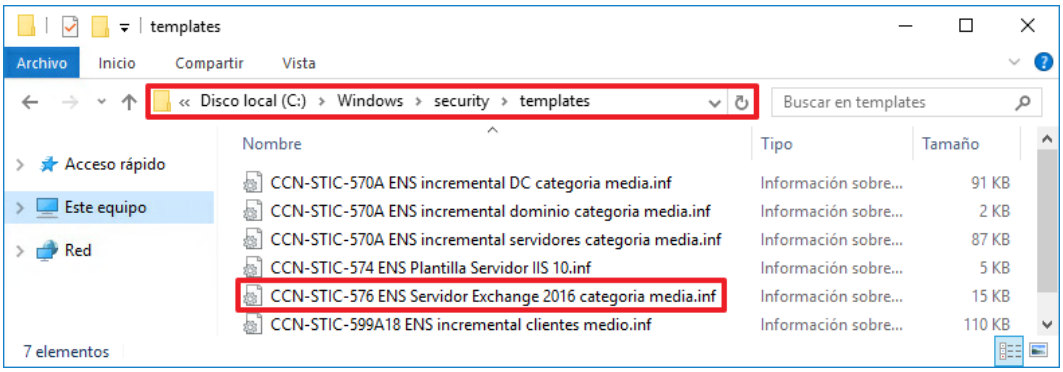
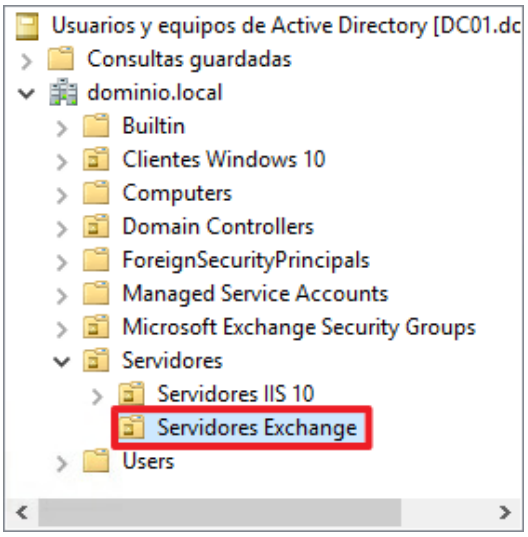
1. PREPARACIÓN DEL DOMINIO

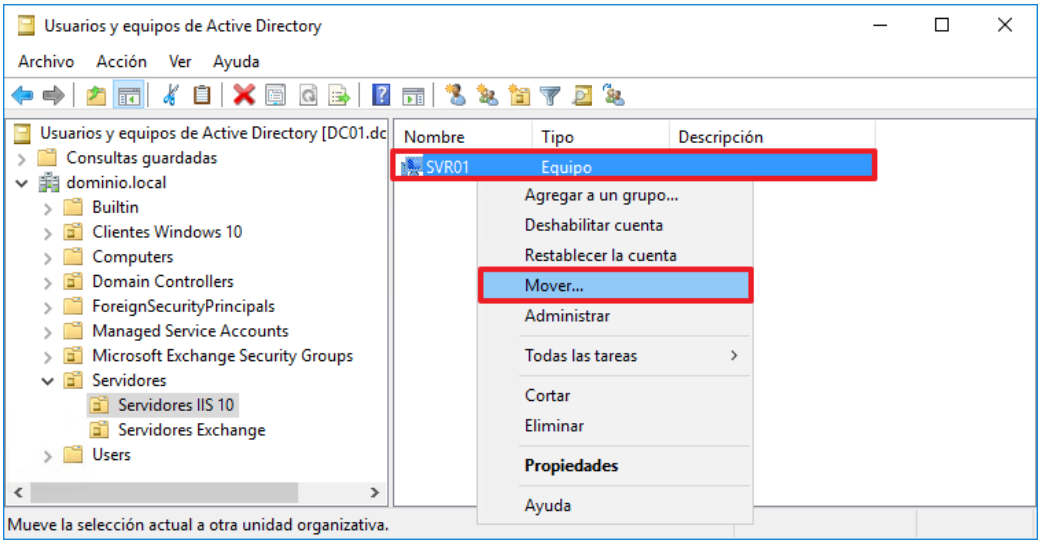
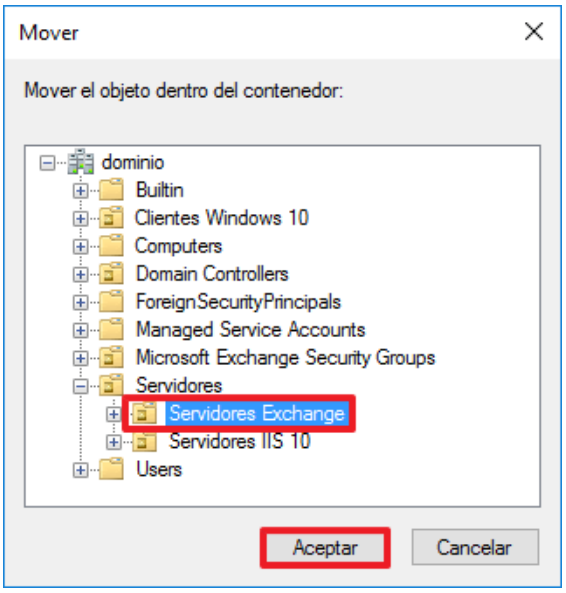
Los pasos que se describen a continuación se realizarán en un controlador del dominio al que va a pertenecer el servidor miembro que contenga Microsoft Exchange Server 2016. Estos pasos sólo se realizarán cuando se incluya el primer servidor de Microsoft Exchange Server 2016 que actúe como miembro del dominio. Durante este procedimiento se crea la unidad organizativa que contiene los servidores de correo y se realizan las configuraciones de políticas de grupo correspondientes.

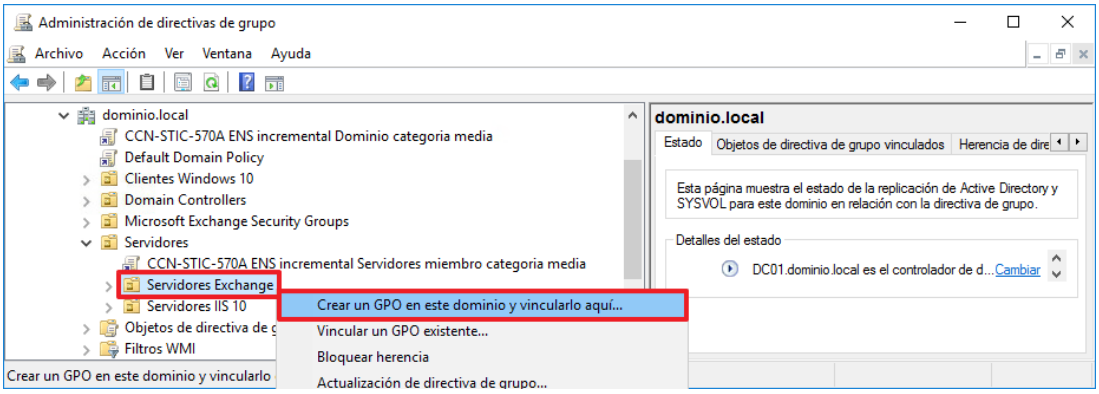
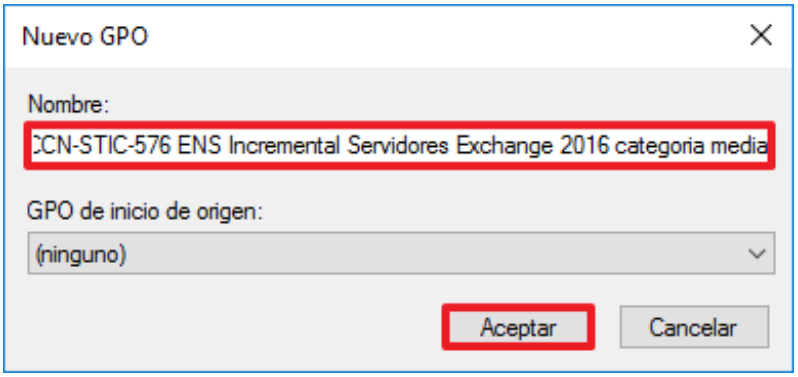
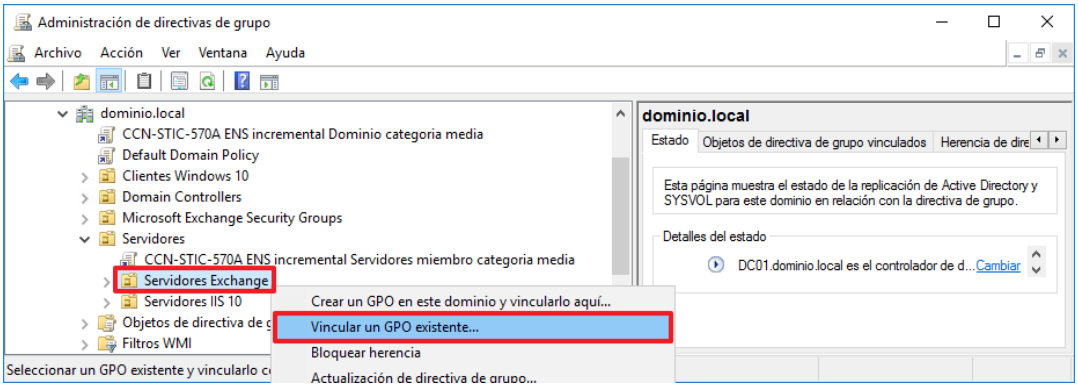
Nota: Esta guía asume que los servidores Controladores del Dominio al que pertenece el equipo servidor de Exchange que está asegurando, se les ha aplicado la configuración descrita en la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016". Si no es así, aplique la guía correspondiente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

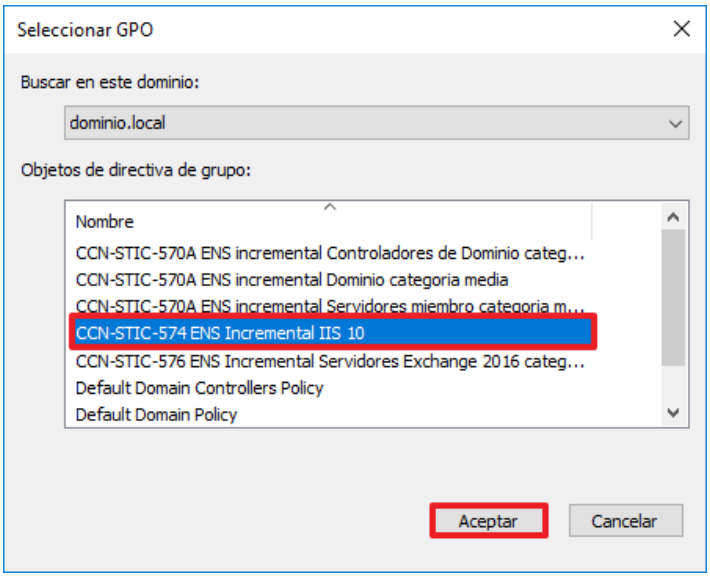
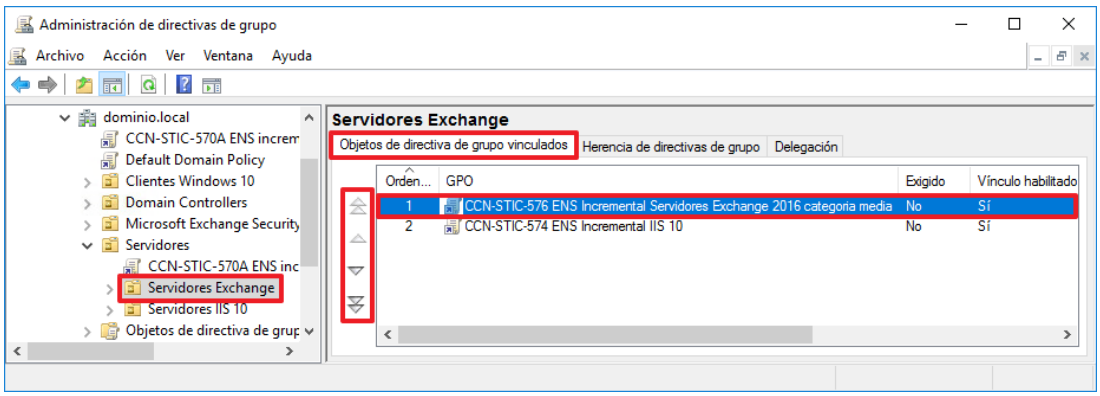
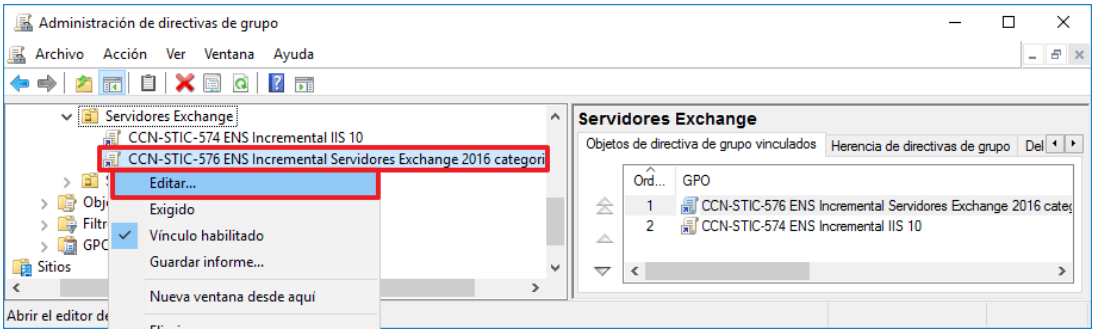
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.

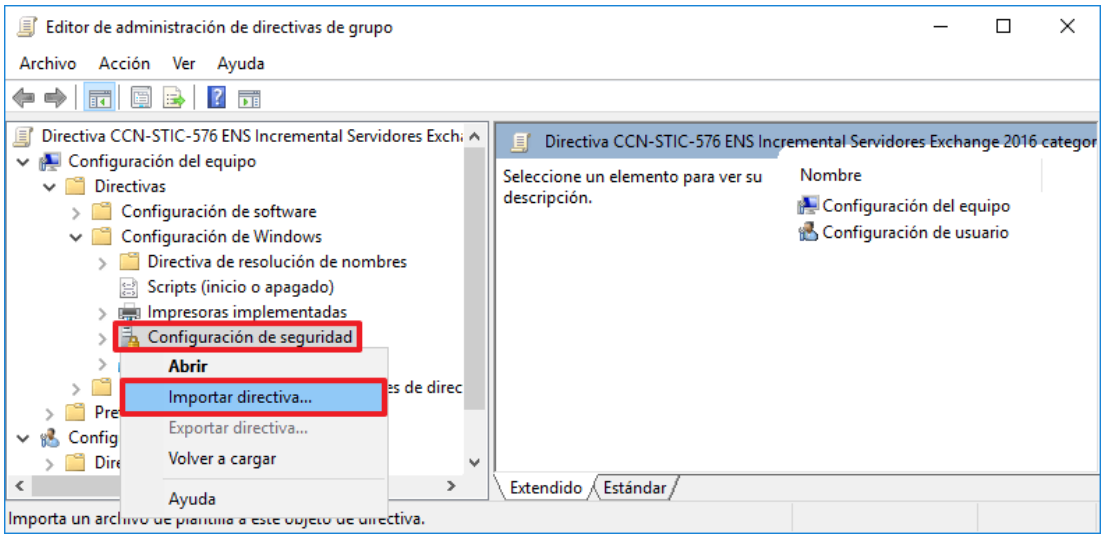
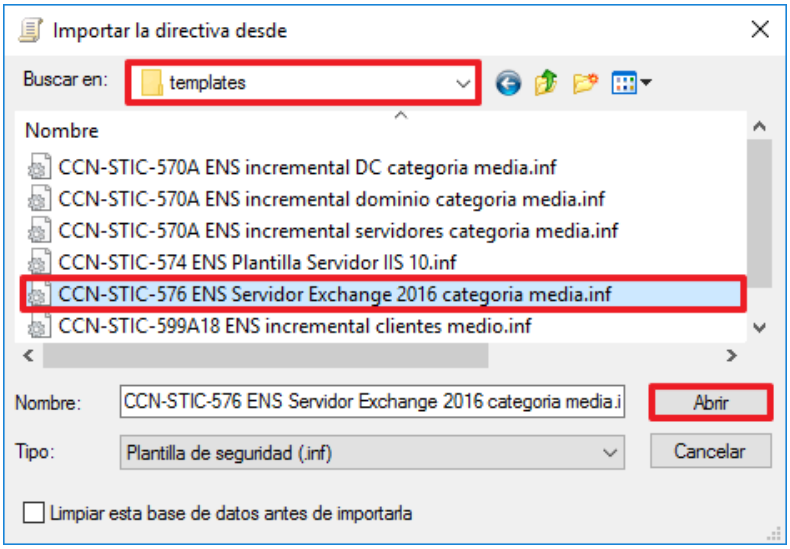
Paso	Descripción
2.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.
4.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos.
5.	Para configurar el “Explorador de Windows” de modo que muestre las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones" de la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

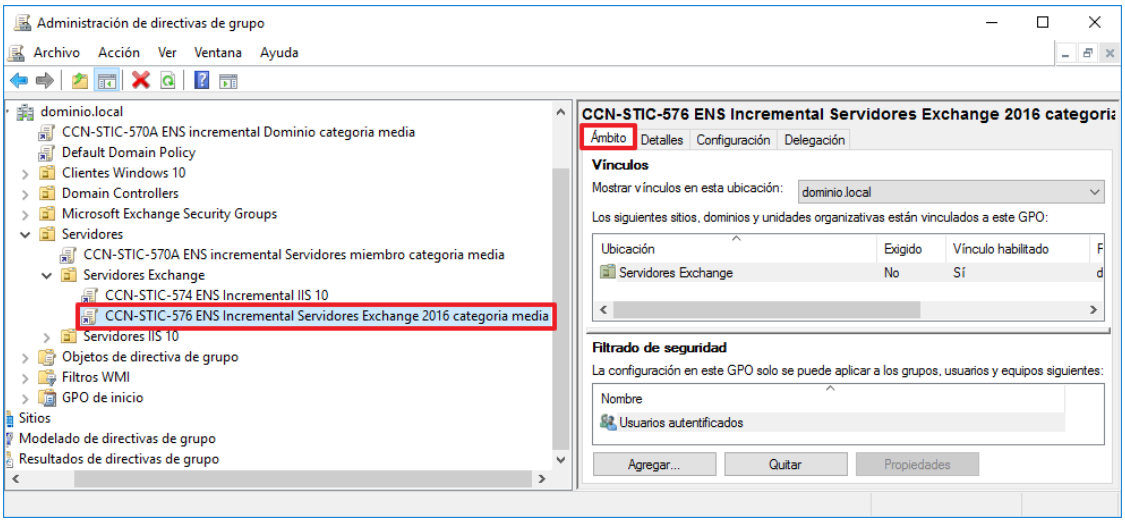
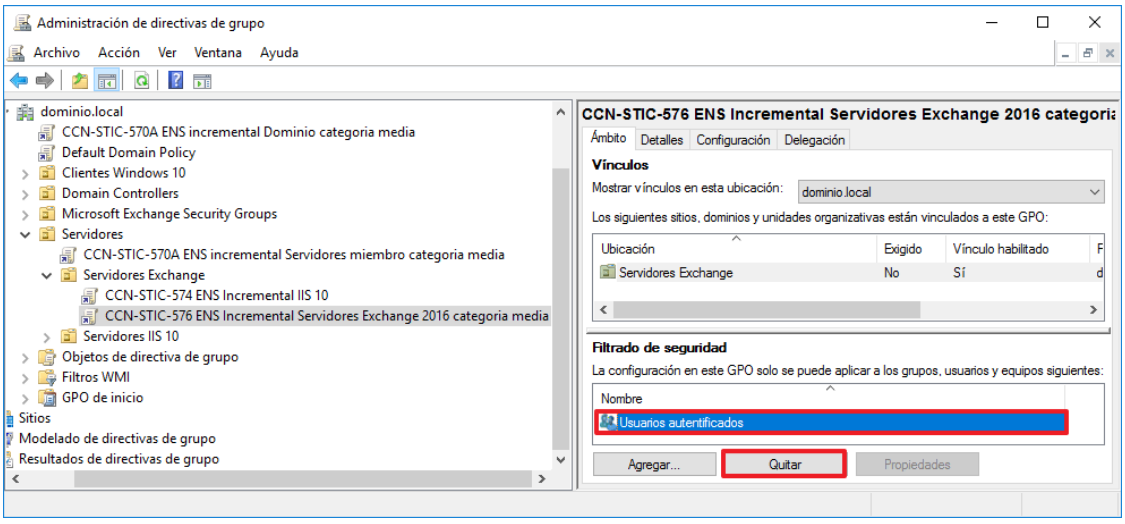
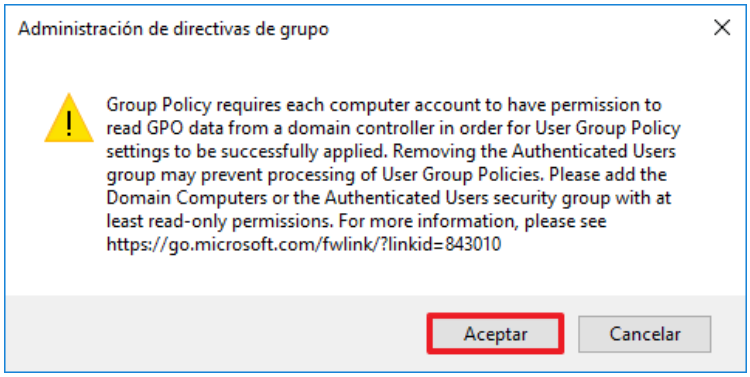
Paso	Descripción
6.	Copie los ficheros "CCN-STIC-576 ENS Servidor Exchange 2016 categoria media.inf" al directorio "C:\Windows\Security\Templates" del Controlador de Dominio.  **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón "Continuar" y pulse "Sí" con una cuenta la cual debe ser al menos administrador de dominio.
7.	Ejecute la consola administrativa Usuarios y Equipos de Directorio Activo desde el Administrador del servidor **"Herramientas → Usuarios y Equipos de Active Directory"**. **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el menú de inicio. Si lo inicia por primera vez, el control de cuentas de usuario le solicitará permiso para iniciar el administrador del servidor.
8.	En la consola, cree una nueva unidad organizativa denominada "Servidores Exchange" dependiendo de la unidad organizativa "Servidores", tal y como se muestra en la imagen.  **Nota:** En este ejemplo se crea la nueva unidad organizativa bajo "Servidores". Modifique este paso de acuerdo con las necesidades del entorno de su organización.

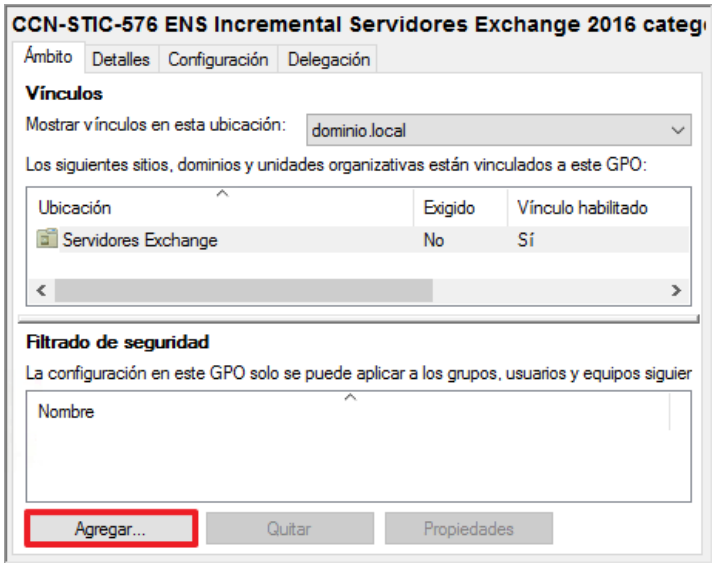
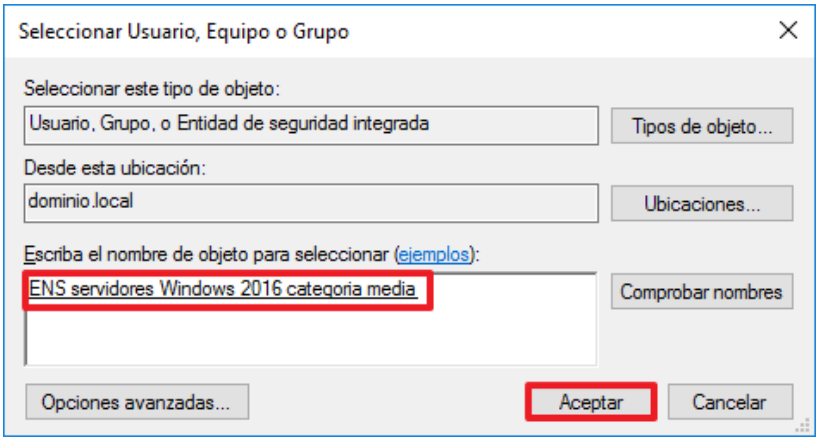
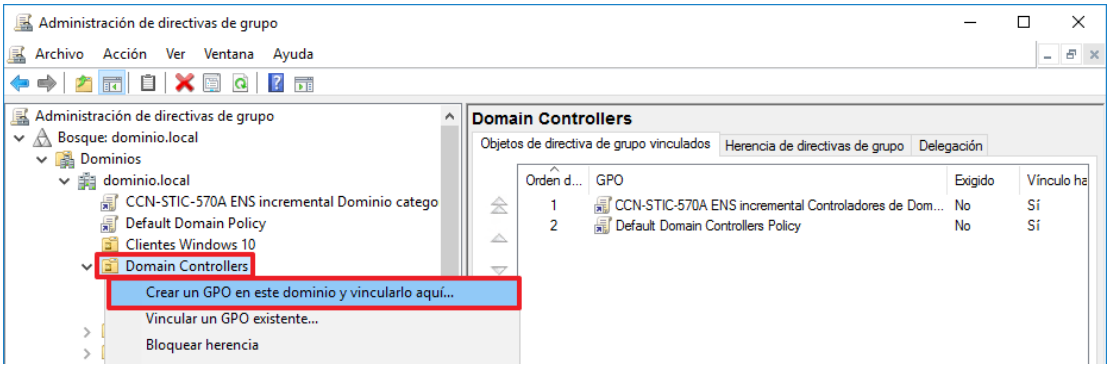
Paso	Descripción
9.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores que contengan Exchange Server 2016 a la unidad organizativa "Servidores Exchange". Para ello, deberá hacer clic botón derecho sobre "Mover" en el servidor que desee ubicar en la nueva unidad organizativa.  **Nota:** Si ha seguido los pasos de la guía "CCN-STIC-574 Implementación del ENS en IIS 10 sobre Windows Server 2016" el servidor se encontrará bajo la unidad organizativa "Servidores IIS 10".
10.	A continuación, seleccione la unidad organizativa "Servidores Exchange". 
11.	Cierre la herramienta de "Usuarios y equipos de Directorio Activo"
12.	Una vez realizada la preparación del Directorio Activo que dará servicio a Exchange Server 2016, deberá realizar el resto de preparación y configuración de políticas de seguridad. Para ello, inicie la consola de administración de directivas de grupo desde el Administrador del servidor en el menú **"Herramientas → Administración de directivas de grupo"**.

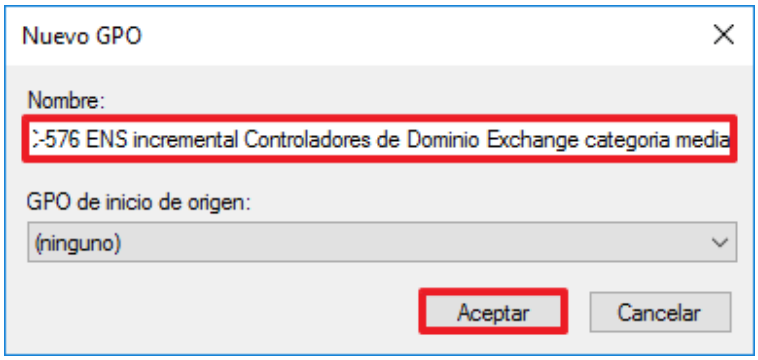
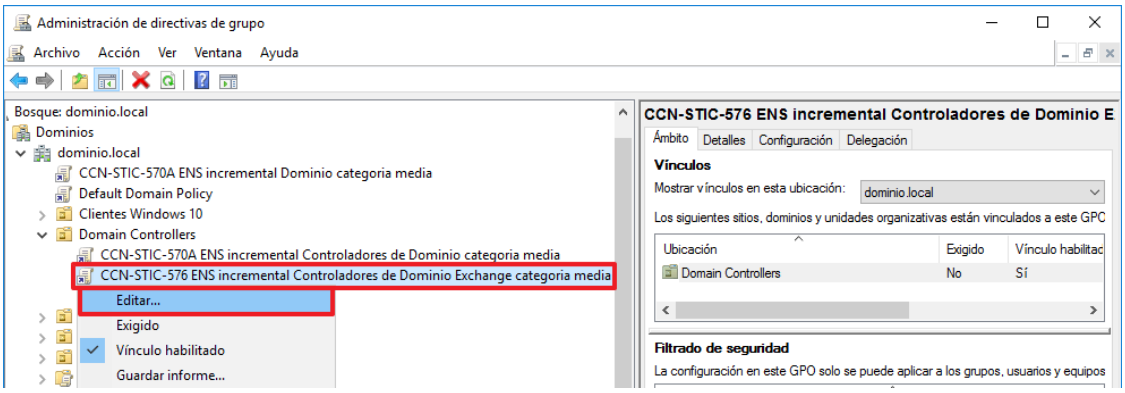
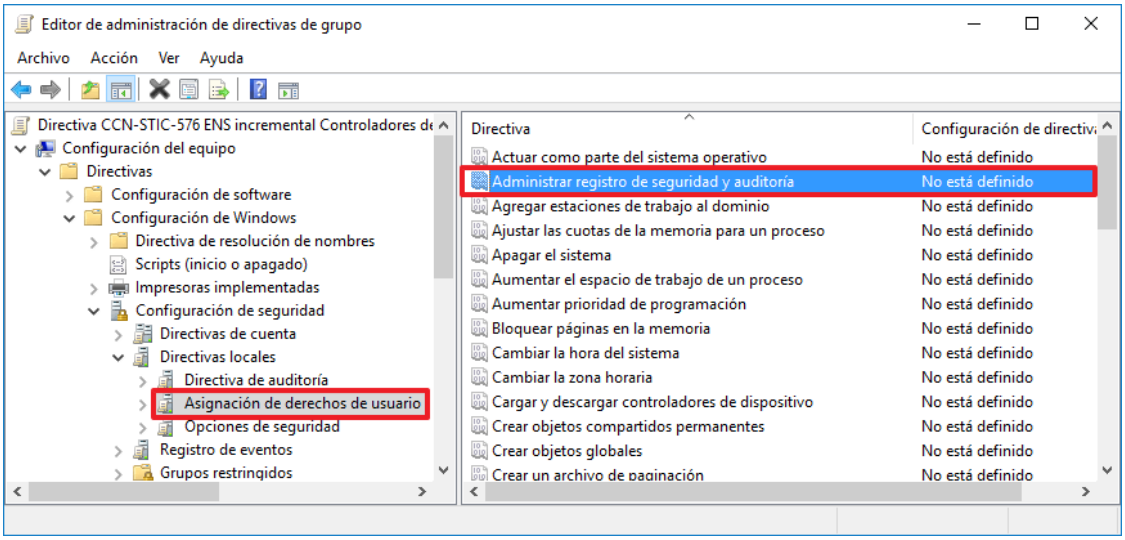
Paso	Descripción
13.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa recién creada "Servidores Exchange", haciendo clic con el botón derecho en el menú "Crear un GPO en este dominio y vincularlo aquí…". 
14.	Escriba el nombre de la GPO "CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria media" y haga clic en el botón "Aceptar". 
15.	A continuación, se va a vincular la GPO "CCN-STIC-574 ENS Incremental IIS 10" de la guía "CCN-STIC-574 Implementación del ENS en IIS 10 sobre Windows Server 2016", en la unidad organizativa "Servidores Exchange" creada en pasos anteriores.
16.	Pulse botón derecho sobre la unidad organizativa "Servidores Exchange" y haga clic sobre "Vincular un GPO existente…". 

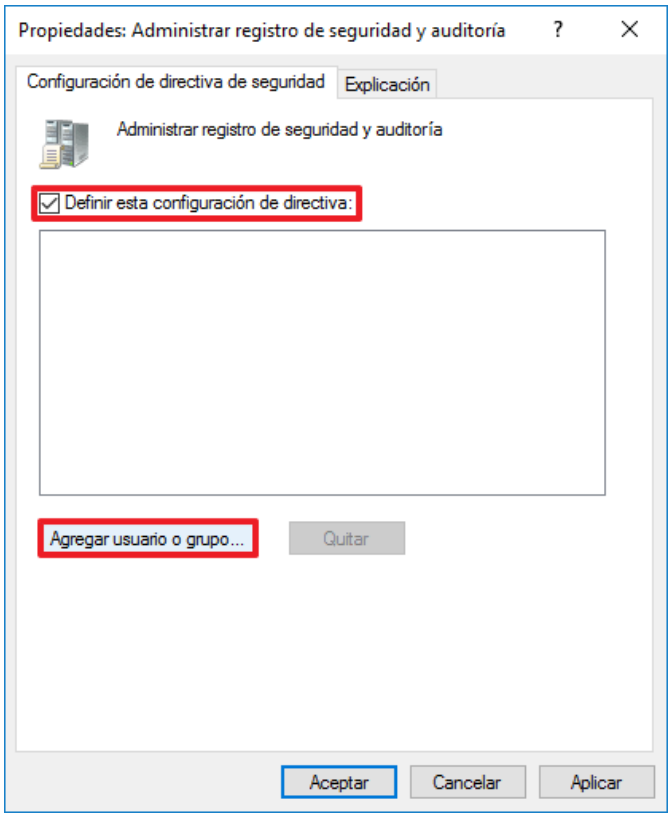
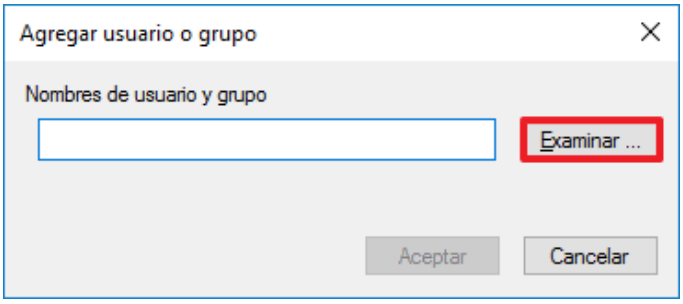
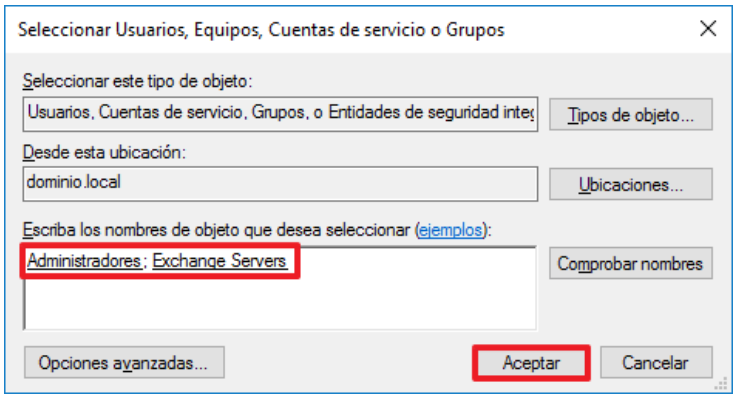
Paso	Descripción
17.	A continuación, seleccione el objeto de directiva de grupo: "CCN-STIC-574 ENS Incremental IIS 10" y pulse sobre "Aceptar". 
18.	Para que la aplicación de las directivas se realice en el orden correcto, asegúrese de que la directiva "CCN-STIC-576 ENS Incremental Servidor Exchange 2016 categoria media" aparezca en primer lugar. Para ello seleccione, dentro de la unidad organizativa, la directiva "CCN-STIC-576 ENS Incremental Servidor Exchange 2016 categoria media" y a continuación, haga clic sobre la flecha doble hacia arriba para que se sitúe en primer lugar del orden vínculos, tal y como se muestra en la imagen. 
19.	A continuación, edite la GPO: "CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria media" creada anteriormente haciendo clic con el botón derecho en ella y seleccionando el menú "Editar". 

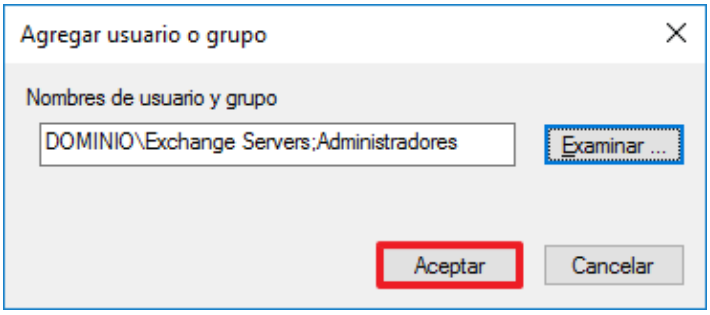
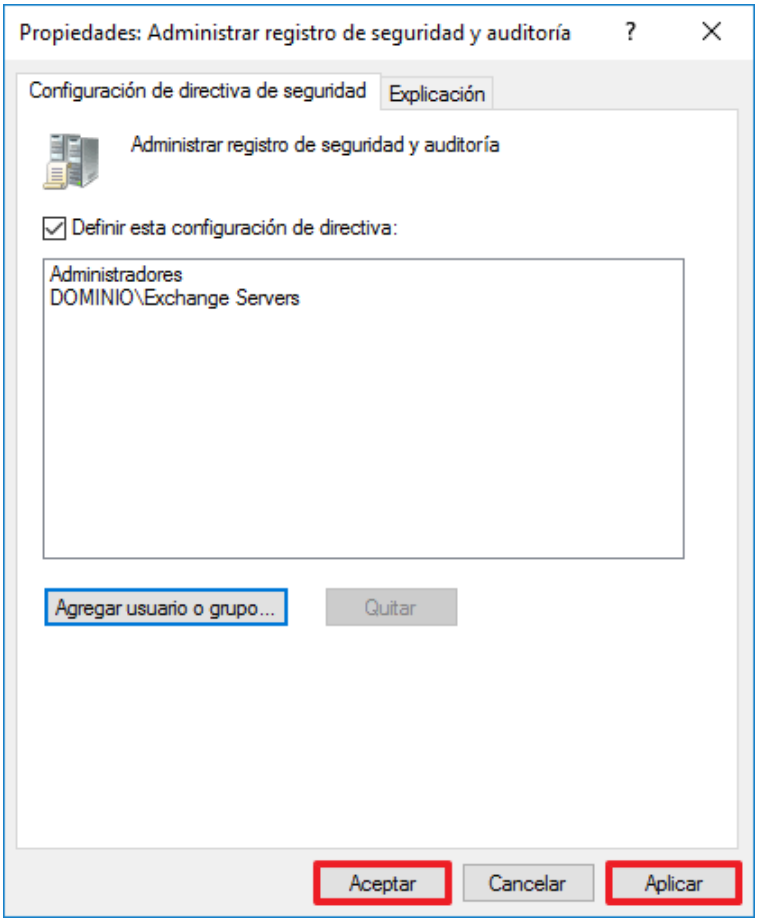
Paso	Descripción
20.	Expanda el nodo **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad"**.
21.	A continuación, haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 
22.	Importe la plantilla de seguridad "CCN-STIC-576 ENS Servidor Exchange 2016 categoria media.inf" que previamente debe haberse copiado en la ruta "C:\Windows\Security\Templates" y haga clic en botón "Abrir". 
23.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.

Paso	Descripción
24.	Seleccione la nueva política de grupo configurada y vaya a la pestaña "Ámbito" que se encuentra en el panel derecho. 
25.	En la opción de filtrado de seguridad, seleccione "Usuarios autentificados" y pulse la opción "Quitar". 
26.	Pulse el botón "Aceptar" cuando le pregunte si desea quitar este privilegio de delegación.
27.	Pulse "Aceptar" sobre la advertencia que se mostrará en una ventana emergente. 

Paso	Descripción
28.	Una vez quitado, pulse el botón "Agregar…". 
29.	Introduzca como nombre "ENS servidores Windows 2016 categoria media". Este grupo corresponde con el generado en la aplicación de la guía codificada como "CCN-STIC-570A". A continuación, pulse el botón "Aceptar".  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.
30.	Pulse con botón derecho sobre la unidad organizativa "Domain Controllers" y seleccione "Crear un GPO en este dominio y vincularlo aquí…". 

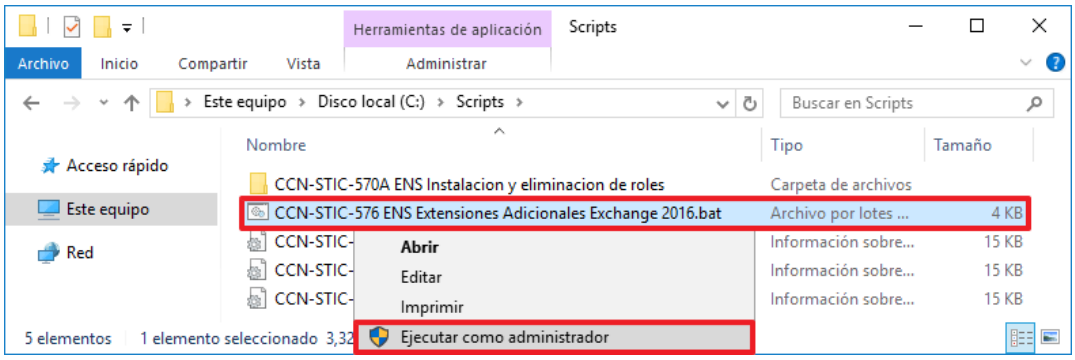
Paso	Descripción
31.	Introduzca el nombre "CCN-STIC-576 incremental Controladores de Dominio Exchange categoria media" y pulse "Aceptar". 
32.	Seleccione la GPO recién creada y pulse "Editar…". 
33.	Despliegue el nodo **"Directiva CCN-STIC-576 incremental Controladores de Dominio Exchange categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"** y haga doble clic sobre la directiva "Administrar registro de seguridad y auditoría". 

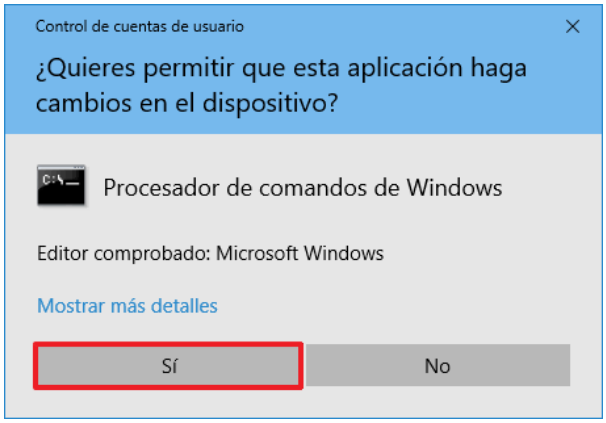
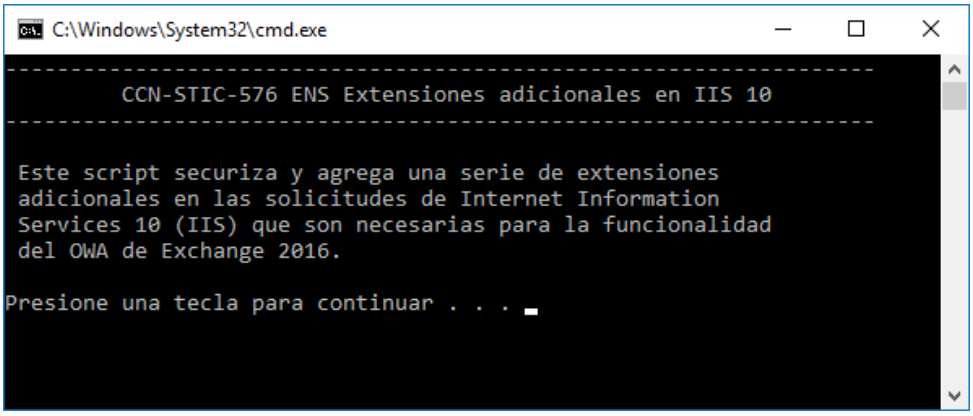
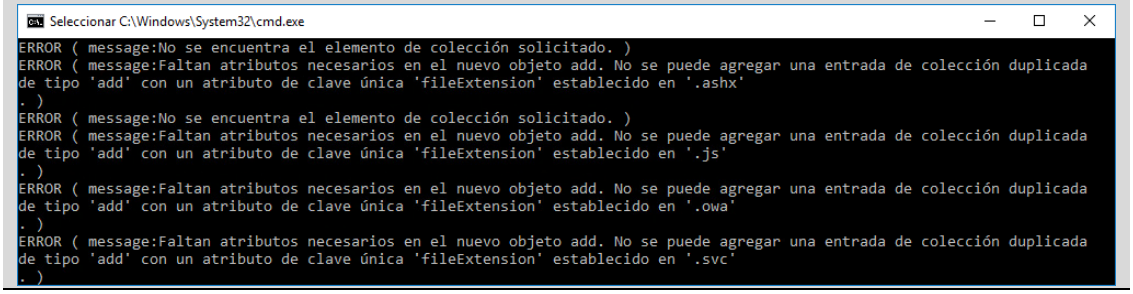
Paso	Descripción
34.	Marque la casilla "Definir esta configuración de directiva:" y pulse sobre "Agregar usuario o grupo…". 
35.	Pulse sobre "Examinar". 
36.	Añada los grupos "Administradores" y "Exchange Servers". Pulse "Aceptar". 

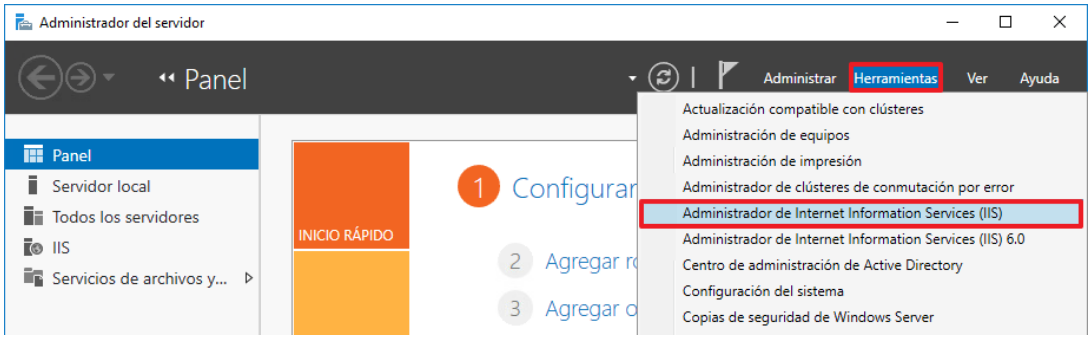
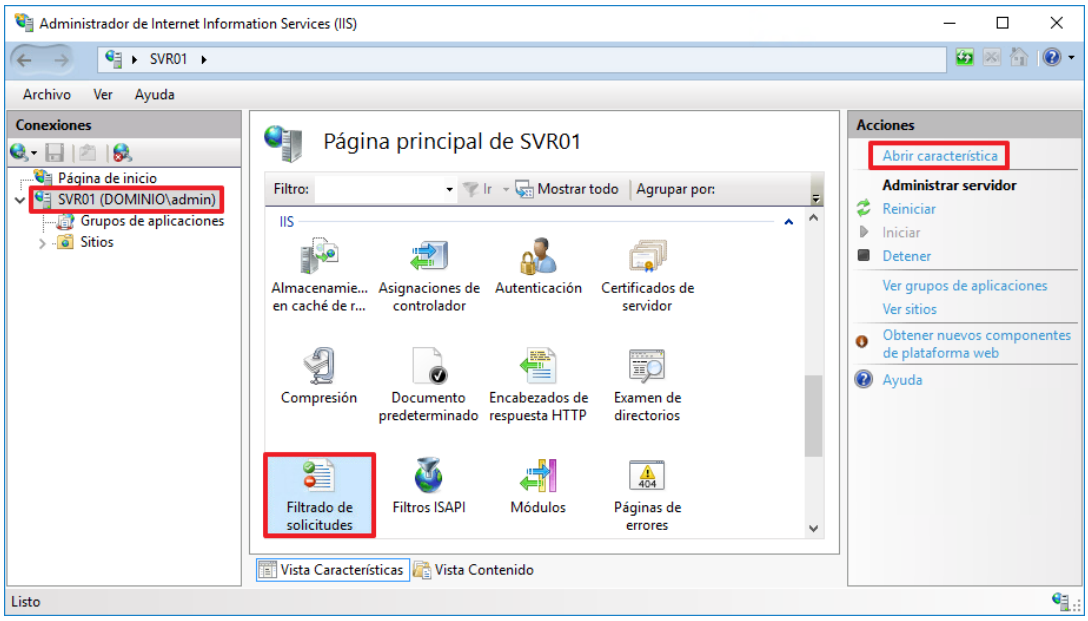
Paso	Descripción
37.	Pulse nuevamente sobre "Aceptar". 
38.	Para finalizar pulse sobre "Aplicar" y "Aceptar". 
39.	Cierre todas las ventanas de administración y borre la carpeta "C:\Scripts".
40.	Reinicie los servidores para que se hagan efectivos los cambios.

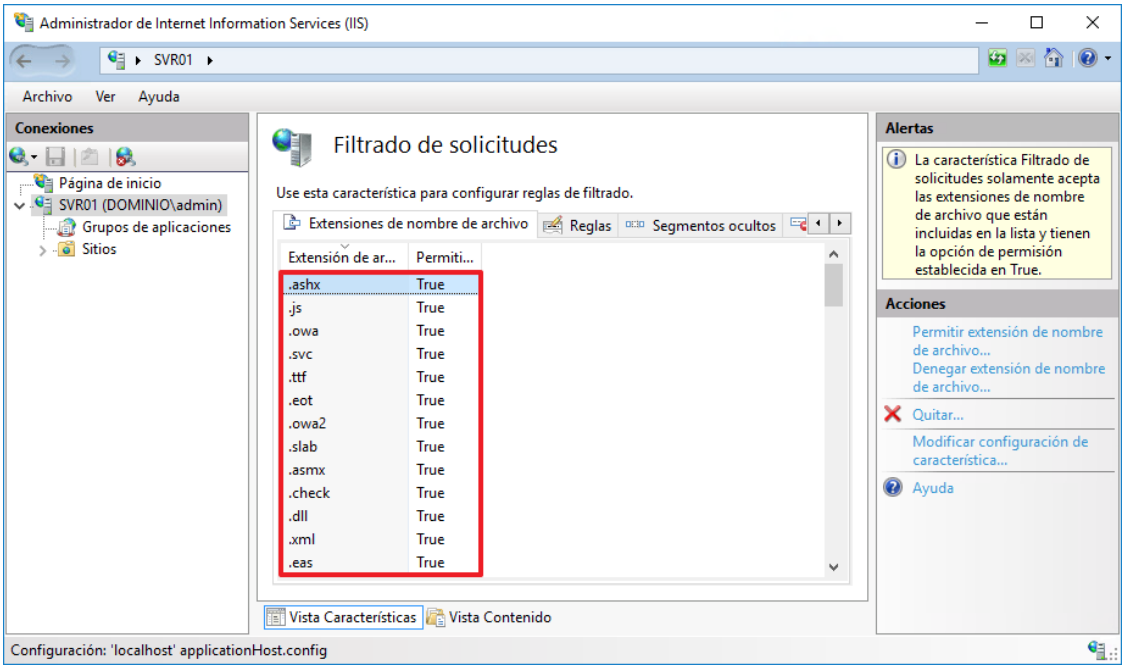
2. PREPARACIÓN DEL IIS 10

Los pasos que se describen a continuación se realizarán en un servidor miembro del dominio al que va a pertenecer el servidor Exchange Server 2016.

Paso	Descripción
41.	Inicie sesión en el servidor miembro donde tenga instalado IIS 10 para agregar las extensiones necesarias para el funcionamiento correcto de Exchange Server 2016.  **Nota:** Deberá iniciar sesión con una cuenta que sea "Administrador del Dominio".
42.	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, tendría que editar los scripts para reflejar la nueva ubicación.
43.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".
44.	Se debe ejecutar el script que permite agregar extensiones al servidor IIS 10. Por lo tanto, con el botón derecho seleccione el fichero denominado "CCN-STIC-576 ENS Extensiones adicionales Exchange 2016.bat" y seleccione "Ejecutar como administrador". 

Paso	Descripción
45.	El control de cuentas de usuario le solicitará elevación de privilegios. 
46.	Aparecerá la siguiente pantalla. Pulse una tecla para continuar.  **Nota:** Si tras la ejecución del script aparece un mensaje de error advirtiendo de que no se puede agregar una entrada de colección duplicada, significa que este procedimiento se ha realizado anteriormente. Omita dicho error y continúe con la ejecución del siguiente paso. 
47.	Cuando haya finalizado la ejecución, pulse una tecla para cerrar la ventana.

Paso	Descripción
48.	Compruebe que se ha aplicado correctamente la configuración de las extensiones, para ello, diríjase al administrador de IIS dentro del desplegable "Herramientas" del "Administrador del servidor". 
49.	Compruebe que se ha aplicado correctamente la configuración de las extensiones, para ello, diríjase al administrador de IIS, seleccione la opción "Filtrado de solicitudes" y en el menú situado en el lateral derecho, pulse "Abrir característica". 

Paso	Descripción
50.	Compruebe que las extensiones de nombre de archivo específicas para Exchange Server 2016 están configuradas correctamente en la columna "Permitido" en "True". Para ello diríjase a la pestaña "Extensiones de nombre de archivo". – .ashx – .js – .owa – .svc – .ttf – .eot – .owa2 – .slab – .asmx – .check – .dll – .eas  **Nota:** En caso de que no aparezca reflejada alguna de las extensiones de nombre de archivo arriba referenciadas, deberá crearlas a mano a través del menú "Acciones" situado a la derecha.
51.	Una vez realizada la comprobación cierre el administrador de Internet Information Services.

3. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

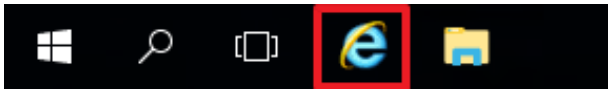
El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto,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

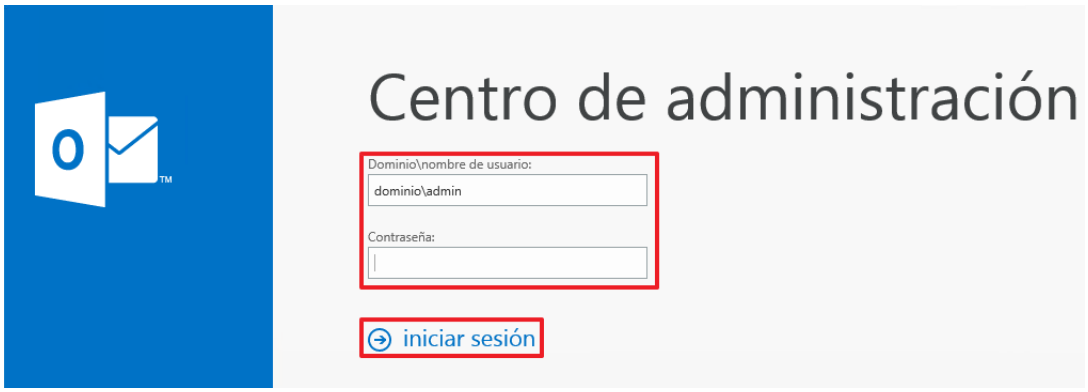
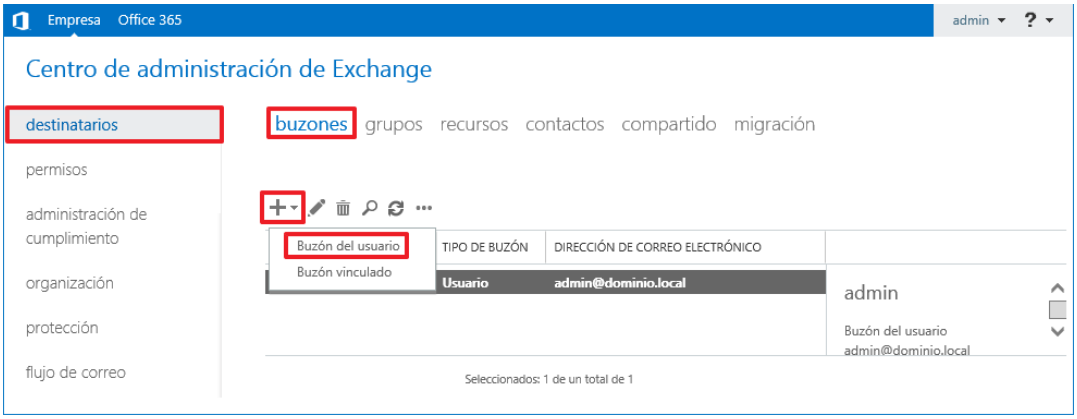
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

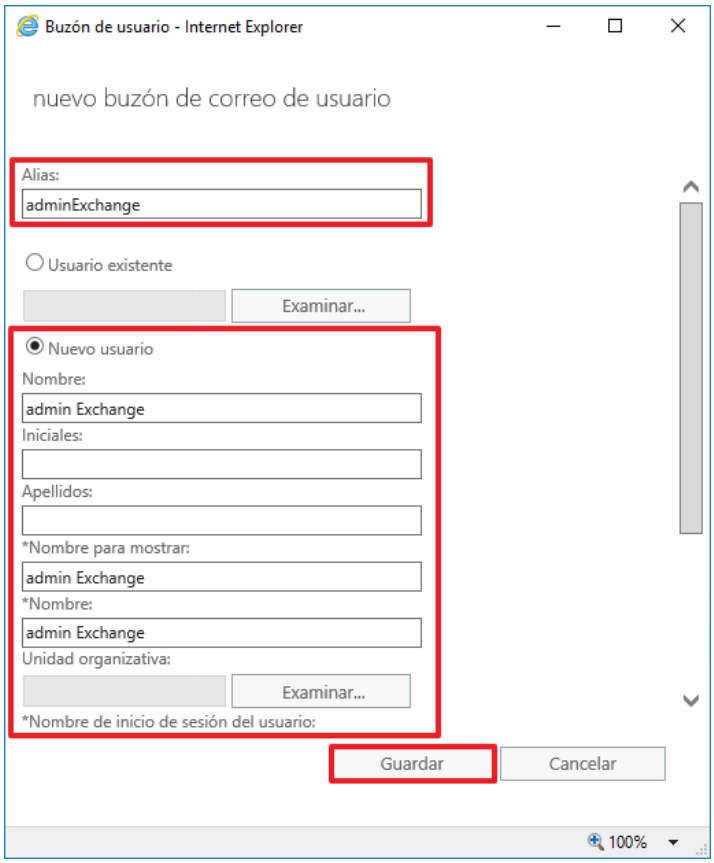
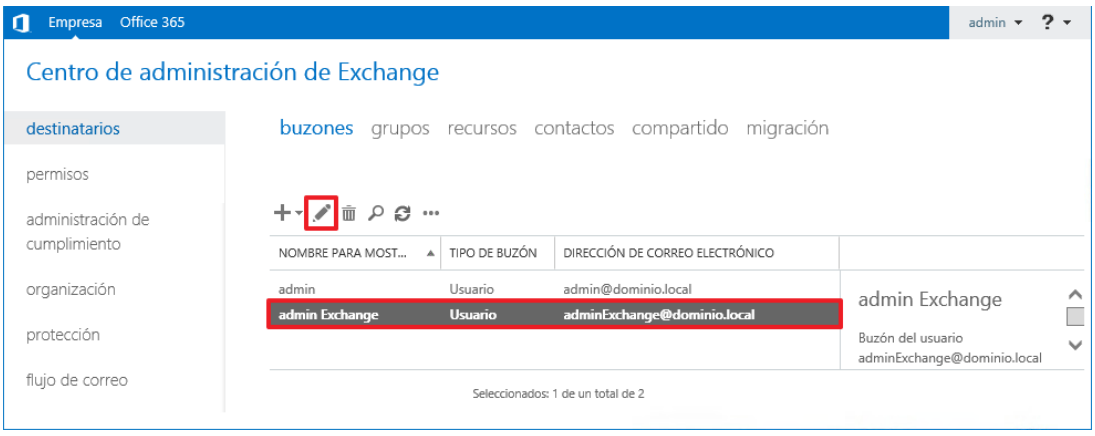
Nota: Todas las recomendaciones de seguridad indicadas en la presente guía deben ser adaptadas al entorno de su organización. Se aconseja realizar las pruebas pertinentes en un entorno de preproducción antes de ser incluidas en su entorno de producción.

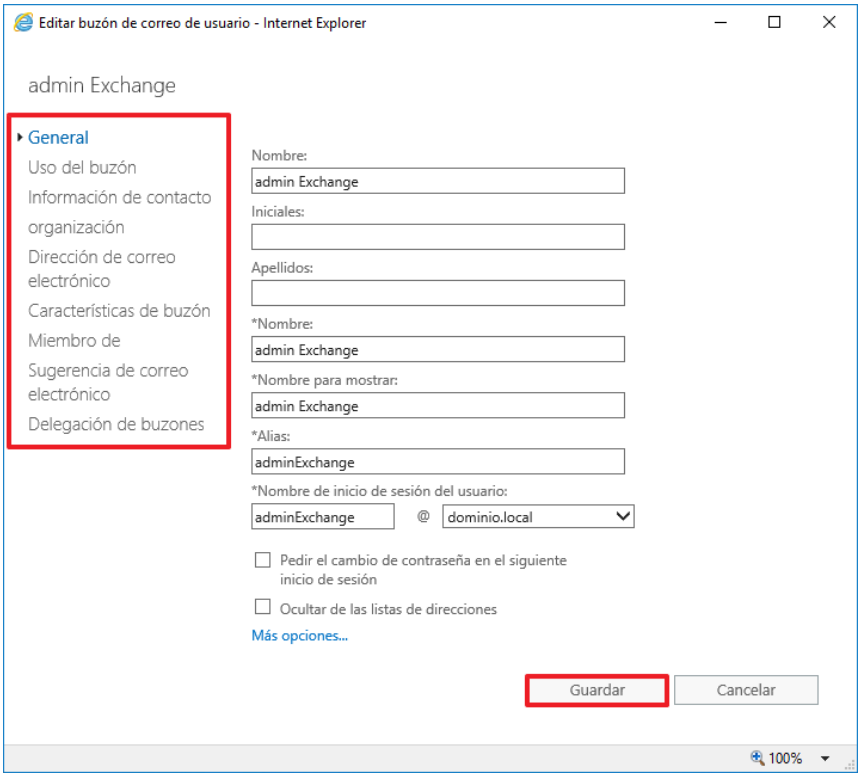
3.1. IDENTIFICACIÓN

Es recomendable que los accesos a los buzones estén completamente controlados y registrados, por ello se deberá usar el directorio activo para la creación de usuarios. Exchange Server 2016 facilita la creación de usuarios de directorio activo integrando en su propio panel de administración toda la creación y gestión del usuario sincronizándose automáticamente con el directorio activo de su organización.

Paso	Descripción
52.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
53.	Pulse sobre "Internet Explorer" en la barra de tareas. 

Paso	Descripción
54.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.
55.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
56.	Seleccione en la pestaña "destinatarios" en la opción de "buzones" un nuevo "Buzón del usuario". 

Paso	Descripción
57.	A continuación, documente los datos del nuevo buzón que desea crear, una vez documentado pulse sobre "Guardar".  **Nota:** También se pueden crear un buzón a un usuario existente en el directorio activo, en este ejemplo se crea un usuario nuevo con su correspondiente buzón.
58.	Una vez creado el nuevo usuario y buzón es posible modificar más características editándolo. Para ello seleccione el buzón que desea editar y pulse "Modificar". 

Paso	Descripción
59.	En la siguiente pantalla puede añadir todos los datos adicionales necesarios para su organización, para ello debe navegar por las diferentes opciones situados en el panel izquierdo. Para finalizar pulse sobre "Guardar". 

3.2. ASIGNACIÓN DE PERMISOS Y ROLES

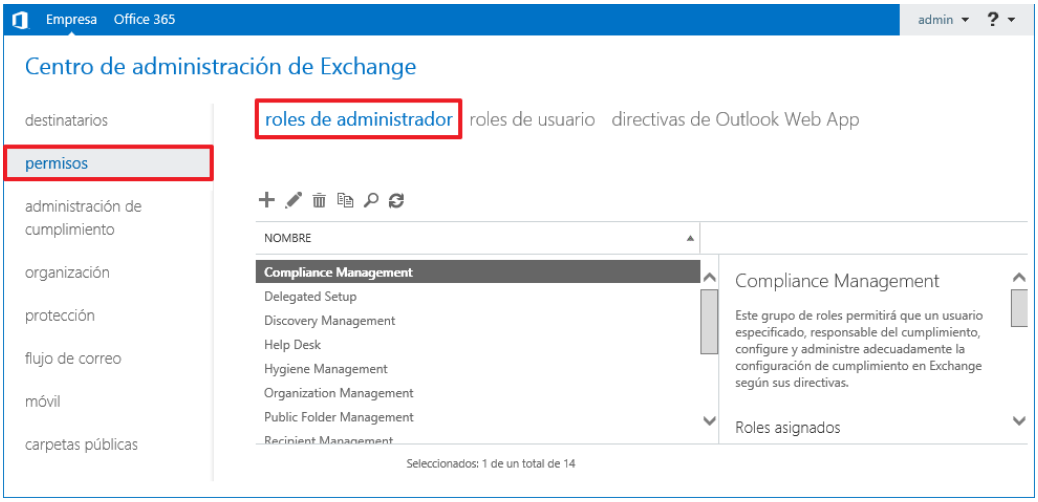
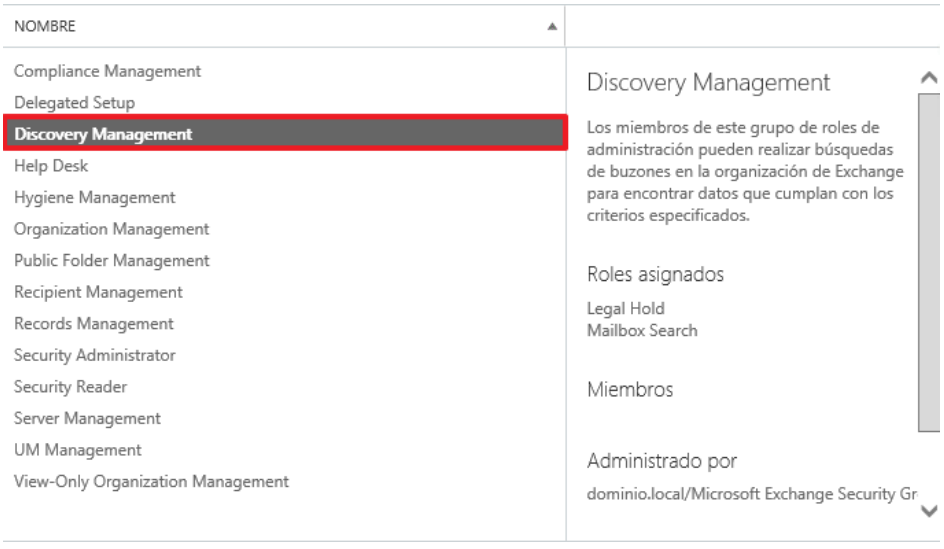
Antes de poder aplicar diferentes mecanismos de auditoría y conformidad, debe tener presente que determinadas funcionalidades requieren de la obtención de permisos específicos para la realización de las operaciones. La asignación de dichos permisos se basa en el modelo RBAC (Role Based Access Control). Dicho modelo tiene su base fundamental en la pertenencia a grupos y a la aplicación de directivas sobre dichos grupos.

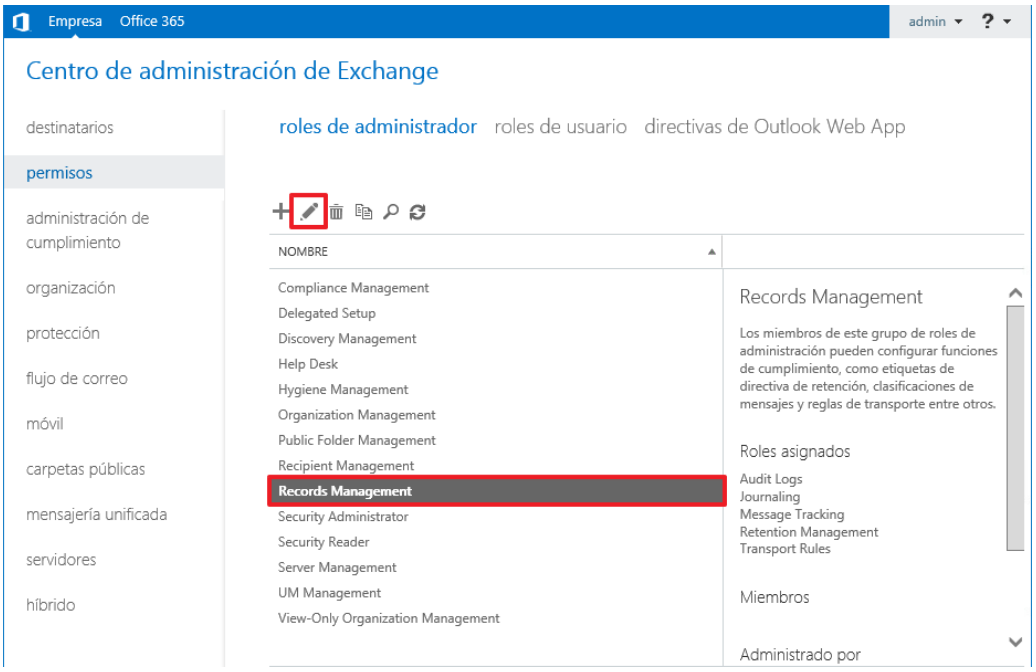
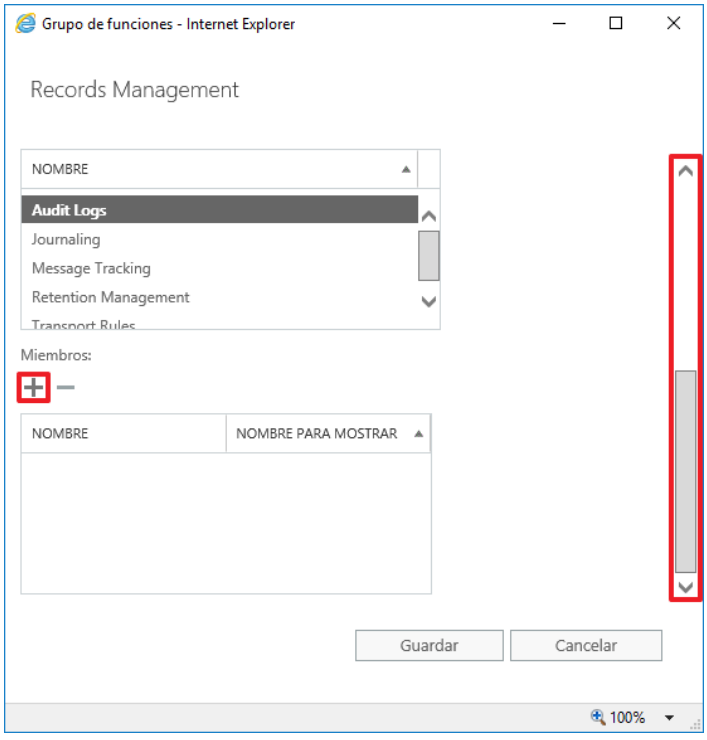
Así mismo, este modelo permite establecer una jerarquía de roles segregados, de tal forma que algunos usuarios de la organización pueden realizar tareas de administración del servidor, a la vez que otros pueden asumir la funcionalidad de auditores del sistema.

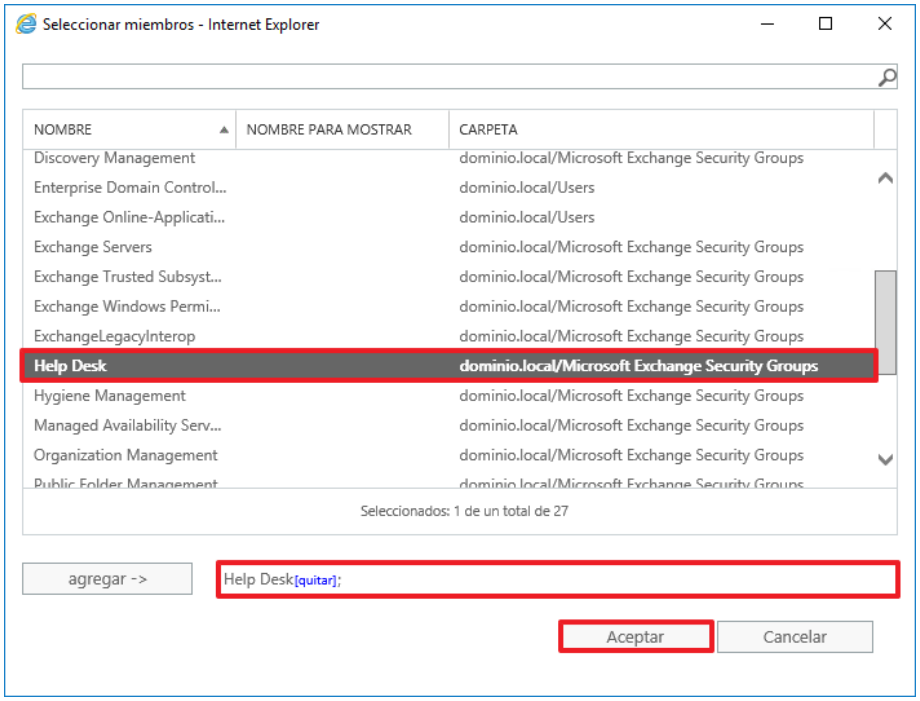
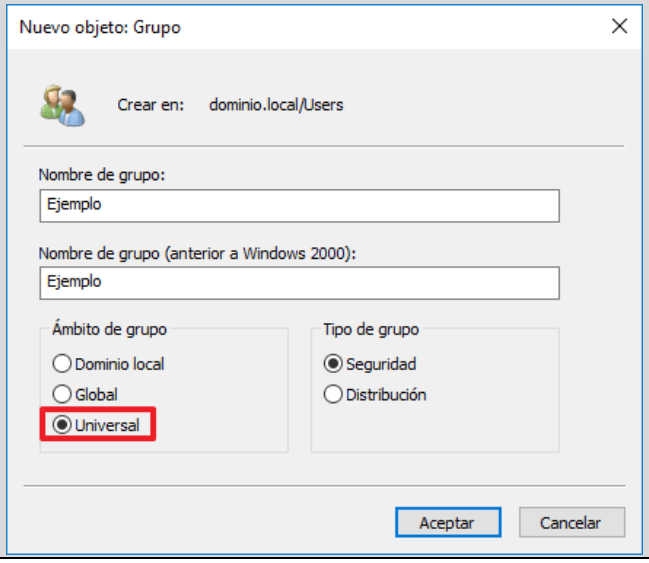
La administración de roles y permisos se puede realizar a través de la consola Web de administración (Exchange Control Panel) o bien a través de cmdlets de PowerShell. Para una mejor comprensión, este anexo mostrará cómo realizar dichas acciones a través del entorno gráfico vía Web.

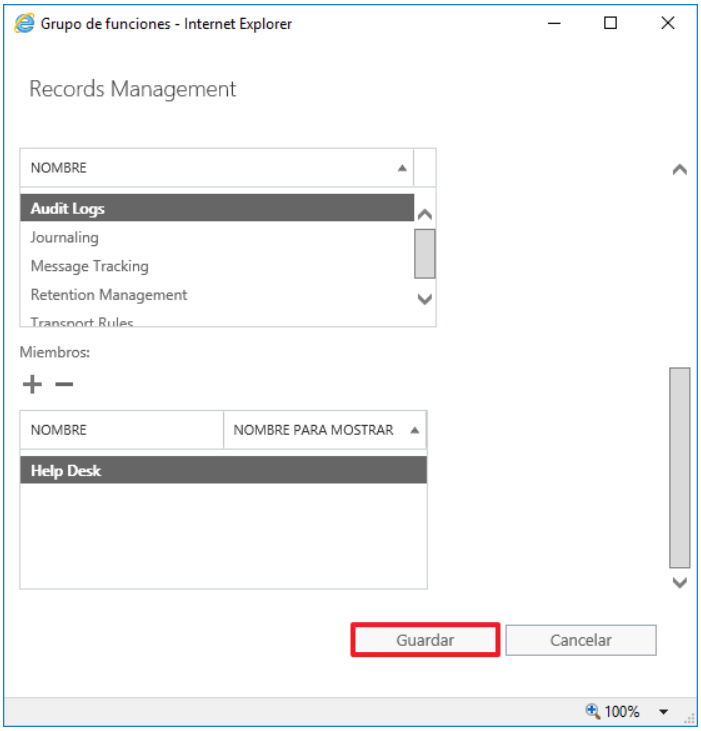
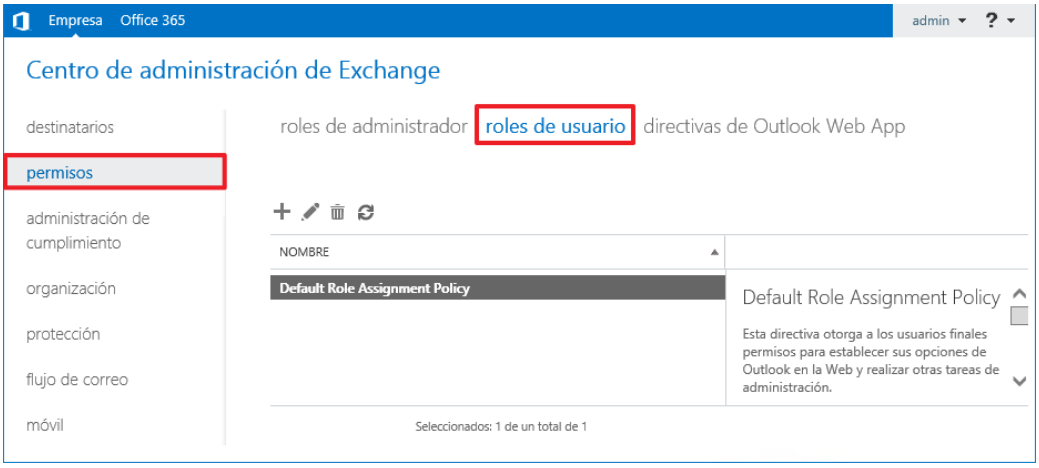
Nota: Si desea crear más información sobre la administración de roles y permisos visite la siguiente web: https://technet.microsoft.com/es-es/library/jj657511(v=exchg.150).aspx.

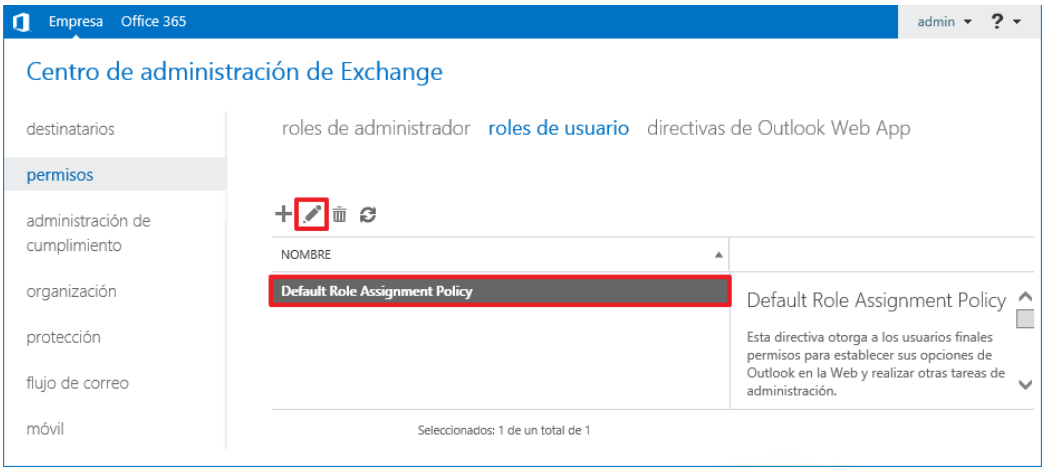
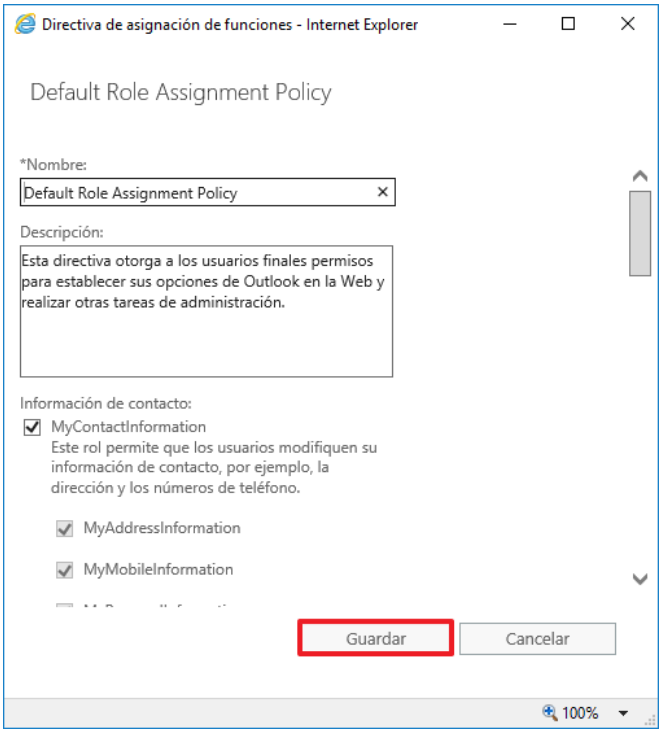
Paso	Descripción
60.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
61.	Pulse sobre "Internet Explorer" en la barra de tareas. 
62.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.
63.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".

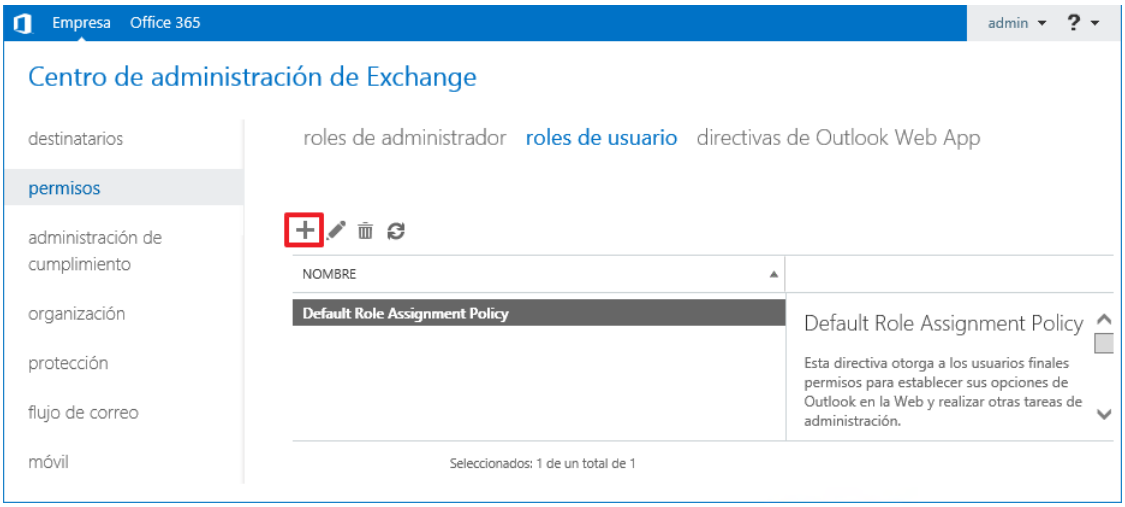
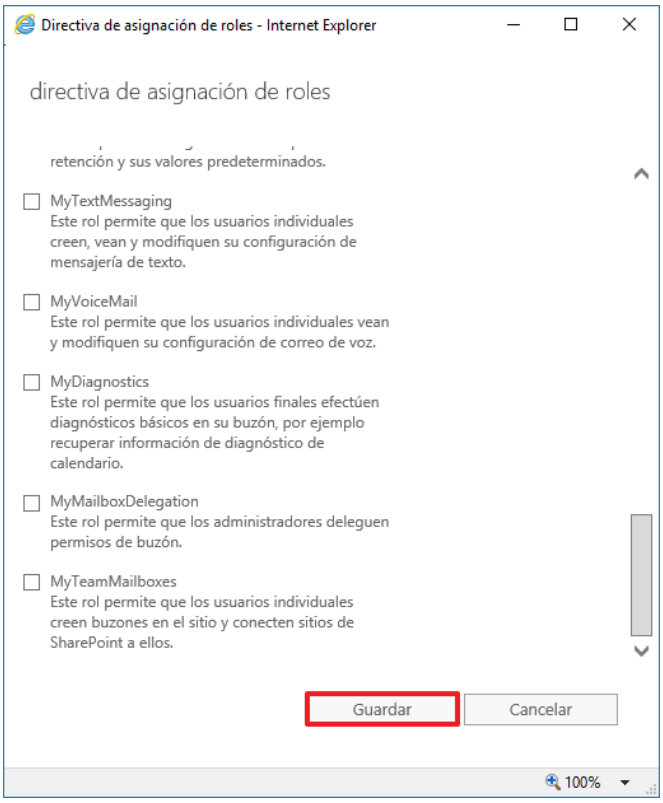
Paso	Descripción
64.	Seleccione el enlace "Permisos" para configurar los permisos RBAC.  **Nota:** Desde este menú se pueden asignar roles de administrador predeterminados a grupos nuevos o existentes en la organización, o también se pueden crear nuevos roles de administrador con permisos específicos.
65.	Por ejemplo, el rol denominado "Discovery Management" o administración de la detección tiene asignados los permisos necesarios para trabajar con la retención legal, así como la suspensión y exhibición de datos electrónicos. Estos permisos incluyen la realización de búsquedas de buzones en la organización para obtener datos que cumplan determinados criterios y la configuración de retenciones legales en los diferentes buzones de correo. 

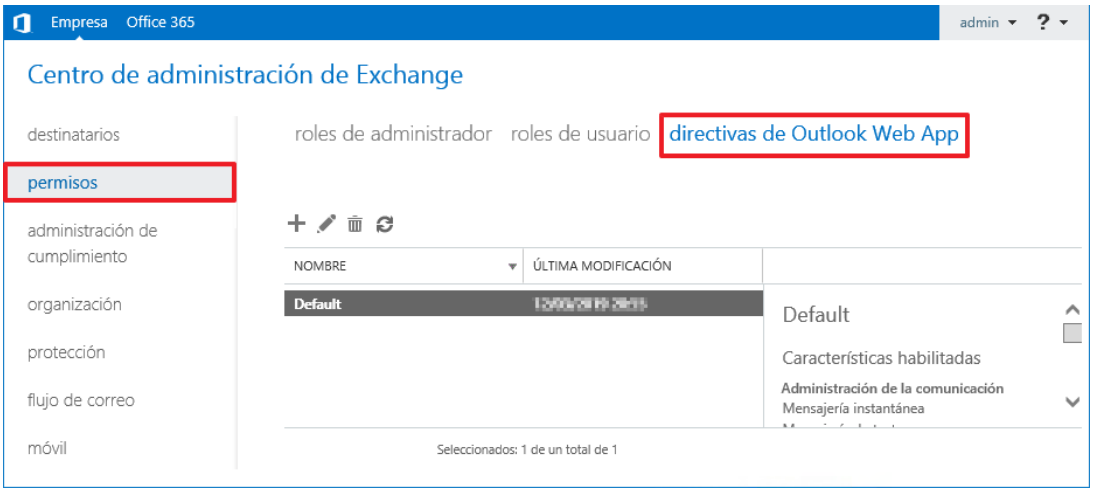
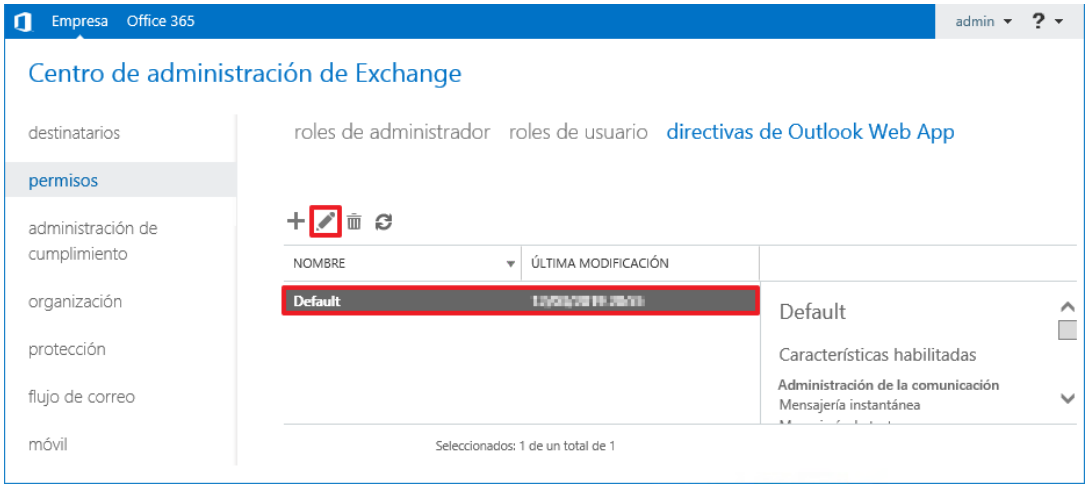
Paso	Descripción
66.	Por otro lado, el rol denominado "Records Management" o administración de registros, incluye otra serie de permisos asignados relativos a las capacidades de auditoría. A continuación, a modo de ejemplo, se va a asignar dicho rol a un grupo de seguridad de Directorio Activo. Para ello, seleccione el rol "Records Management" y pulse el botón "Modificar". 
67.	A continuación, en la sección "Miembros", podrá agregar un grupo de seguridad de Directorio Activo pulsando en el botón "+". 

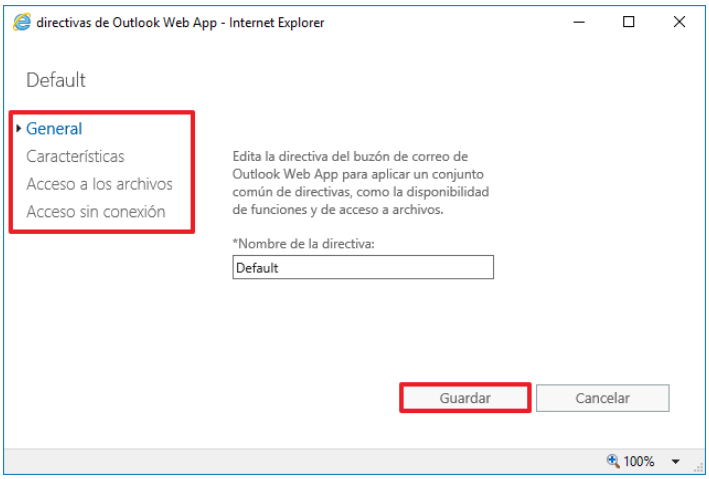
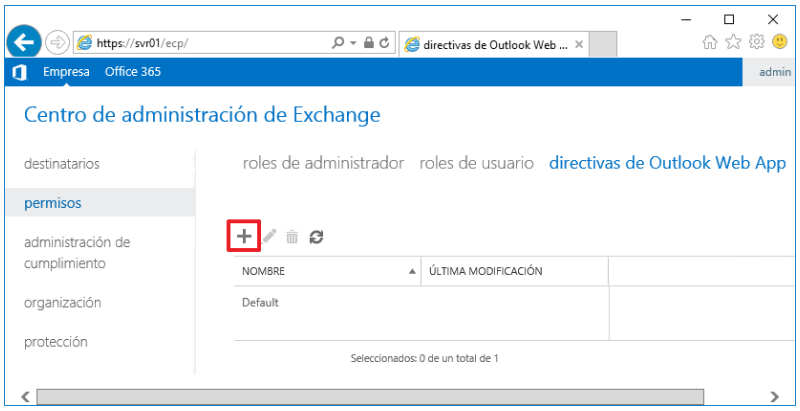
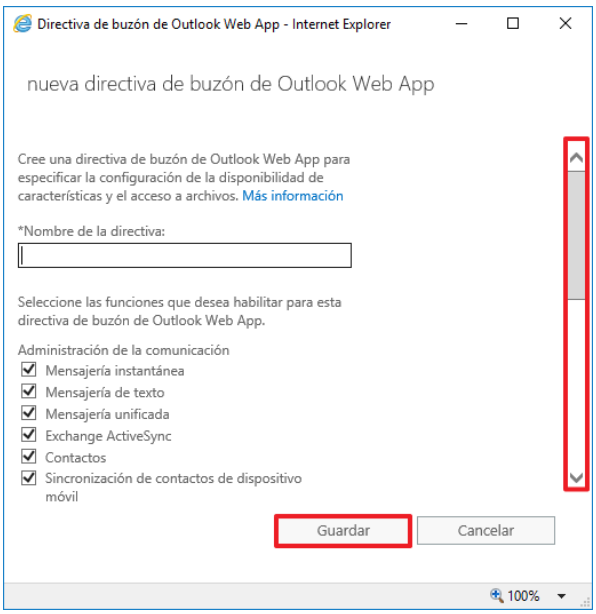
Paso	Descripción
68.	En la pantalla de selección, localice las cuentas de usuarios o grupos de seguridad universales que se desean añadir y pulse el botón "Agregar". Por ejemplo, seleccione el grupo "Help Desk" y pulse en el botón "agregar" y "aceptar".  **Nota:** Para que los grupos de seguridad del Directorio Activo aparezcan en esta ventana de selección, deben ser grupos universales. Los grupos globales o locales no serán visibles. 

Paso	Descripción
69.	A continuación, pulse sobre el botón "Guardar" para hacer efectivos los cambios. 
70.	A continuación, también puede crear grupos de roles de usuario para ello diríjase a la pestaña "permisos" y después a la pestaña "roles de usuario". 

Paso	Descripción
71.	Es posible modificar el grupo de roles de usuario por defecto, pulse sobre el grupo "Default Role Assignment Policy" y a continuación, seleccione "Modificar". 
72.	A continuación, se pueden modificar los campos que sean necesarios para adaptarlos a los requerimientos de su organización y pulse "Guardar". 

Paso	Descripción
73.	Del mismo modo es posible crear un grupo de roles de usuario nuevo, para ello seleccione la pestaña "roles de usuario" pulse sobre la opción nuevo o "+". 
74.	A continuación, cumplimente los campos en función de las necesidades de su organización y pulse "Guardar". 

Paso	Descripción
75.	Del mismo modo puede cambiar las directivas de Outlook Web App, para ello diríjase a la opción "directivas de Outlook Web App". 
76.	A continuación, seleccione la opción que viene creada por defecto, para ello seleccione "Default" y pulse el icono "Modificar".  **Nota:** El valor predeterminado de directiva de buzón de correo de Outlook Web App tiene todas las opciones habilitadas de forma predeterminada.

Paso	Descripción
77.	Cumplimente los campos en función de las necesidades de su organización y pulse "Guardar". 
78.	Si desea crear un grupo de directivas nuevo, debe pulsar sobre nuevo o "+". 
79.	Rellene los campos en función de las necesidades de su organización y pulse "Guardar". 

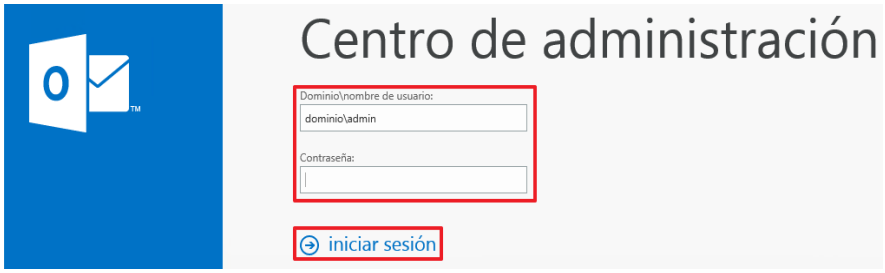
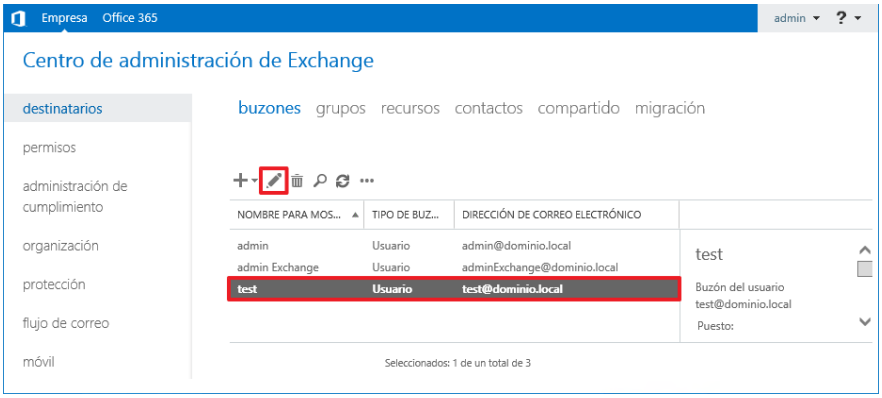
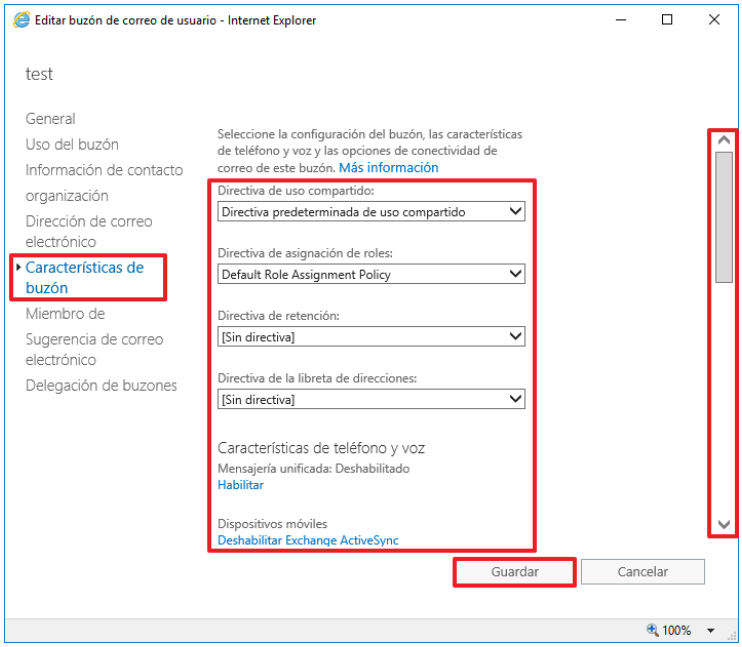
3.3. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

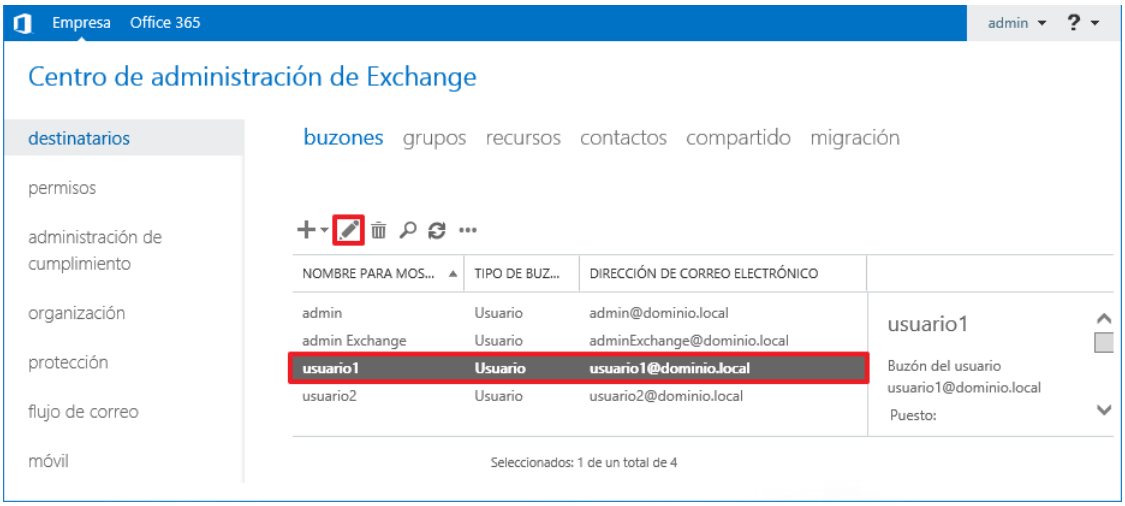
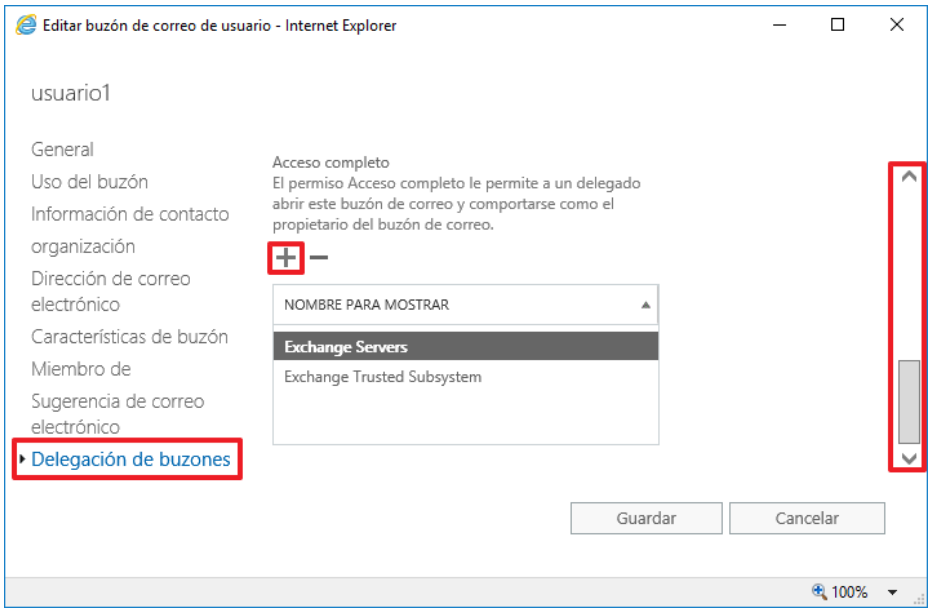
Uno de los aspectos que marca el ENS, desde su requisito de categoría media en el Marco Operacional, es la mínima funcionalidad y mínima exposición evitando con ello posibles vulnerabilidades minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es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

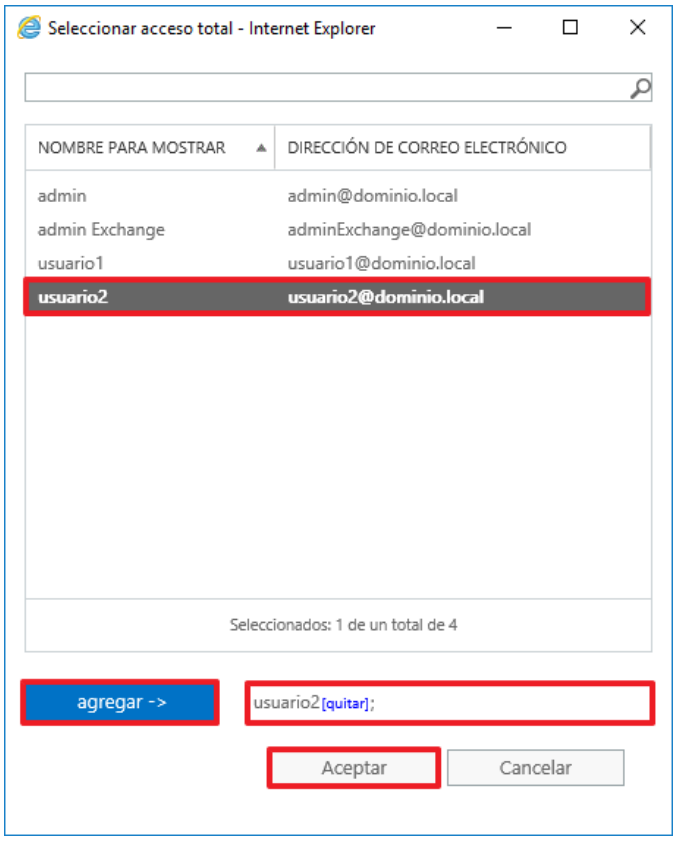
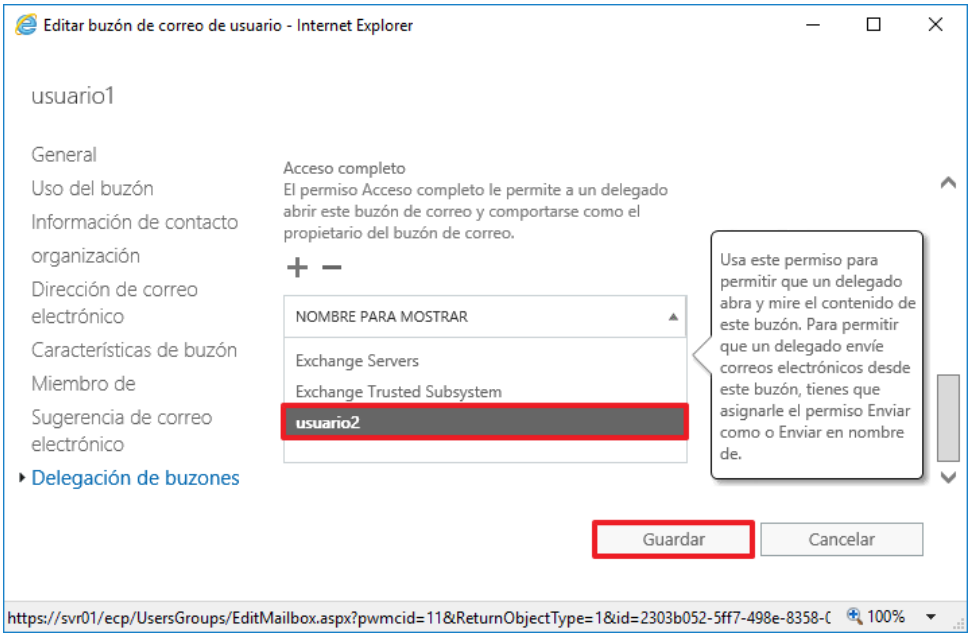
Microsoft Exchange Server 2016 instala por defecto las mínimas funcionalidades para el uso correcto de su producto, por lo que no es posible desinstalar características ya que conllevaría un mal funcionamiento del producto.

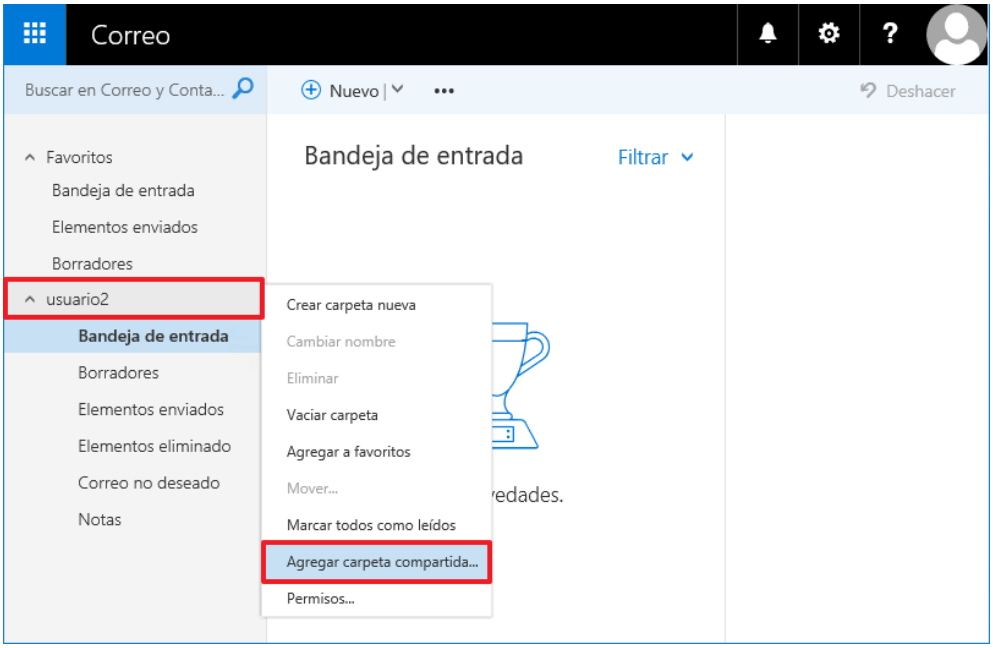
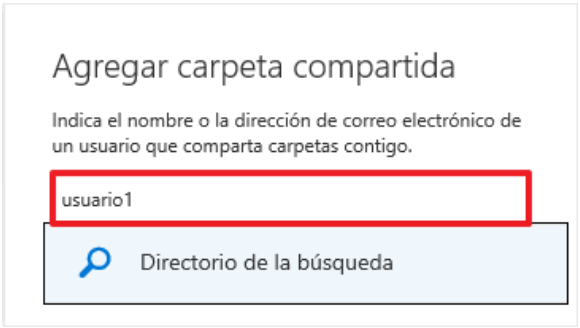
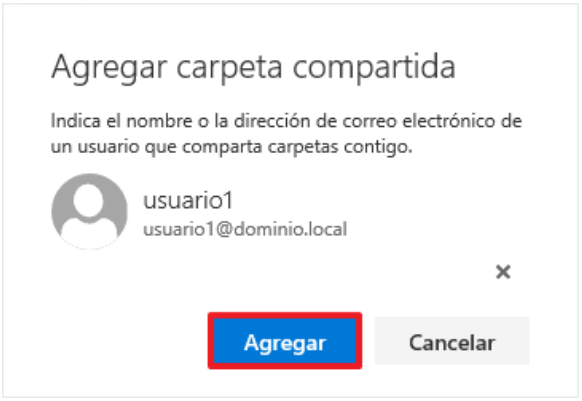
Microsoft Exchange Server 2016 por defecto deshabilita diferentes funcionalidades para aplicar seguridad en el entorno, por ejemplo, los servicios de POP3 e IMAP vienen deshabilitados por lo que si es necesario para su entorno deberá habilitarlo manualmente.

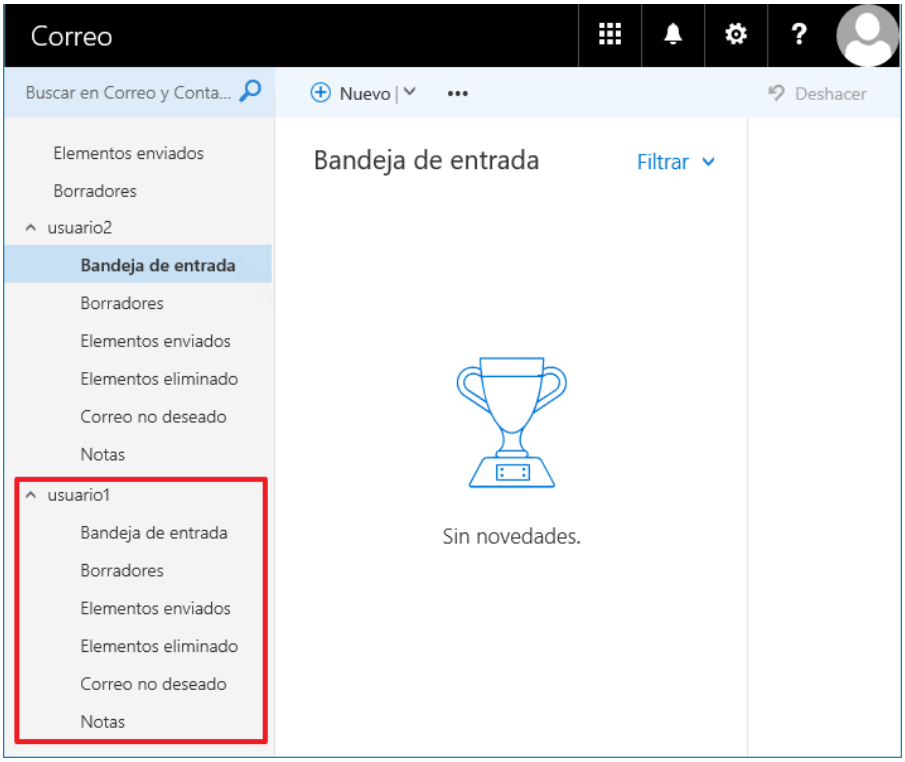
Paso	Descripción
80.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
81.	Pulse sobre "Internet Explorer" en la barra de tareas. 
82.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.

Paso	Descripción
83.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
84.	Seleccione el usuario o buzón en el que desea modificar alguna de las funcionalidades editándolo. Para ello seleccione el buzón que desea editar y pulse "Modificar".  **Nota:** En este ejemplo se usa la cuenta "test". Deberá adaptar los pasos de acuerdo a las necesidades de su organización.
85.	Localice en el menú lateral izquierdo, la opción de "Características de buzón" y seleccione la configuración de buzón según las necesidades de su organización. 

Paso	Descripción
86.	Una característica de seguridad configurable es la posibilidad que un usuario tenga acceso a un buzón de otro usuario, para ello se debe primero conceder los permisos necesarios para acceder al buzón. Seleccione el buzón al que desea acceder con otro usuario y pulse editar.  **Nota:** Para poder realizar este ejemplo se han creado previamente dos buzones, usuario1 y usuario2.
87.	A continuación, desplácese hacia abajo hasta localizar la característica "Acceso completo" dentro del menú "Delegación de buzones" y pulse el botón "Agregar". 

Paso	Descripción
88.	Seleccione el usuario al que desea dar acceso al buzón, pulse "agregar ->" y "Aceptar". 
89.	Compruebe que se ha añadido al usuario dentro de "Acceso Completo". Para finalizar, pulse "Guardar". 

Paso	Descripción
90.	Para comprobar la correcta configuración, inicie sesión en el buzón del "Usuario2", pulse botón derecho sobre una carpeta, y seleccione "Agregar carpeta compartida...".  **Nota:** En este ejemplo se ha usado la cuenta de correo "Usuario2". Adapte estos pasos a los más convenientes para su organización.
91.	A continuación, escriba el usuario o el buzón que desee agregar. 
92.	Una vez seleccionado el usuario pulse "Agregar". 

Paso	Descripción
93.	Compruebe que tiene acceso al nuevo buzón agregado. 

3.4. MECANISMOS DE AUTENTICACIÓN

En Microsoft Exchange Server 2016 la autenticación básica establecida por defecto se realiza con usuario y contraseña gracias a la integración con el directorio activo de su organización asegurando que las contraseñas cumplan con los requisitos mínimos que se establecen en el ENS, por lo que se deben asegurar en la categoría media del marco operacional unas claves seguras.

En la categoría media del marco operacional del ENS se recomienda no usar claves concertadas, aunque si está permitido su uso.

En la categoría alta - DL del marco operacional del ENS se recomienda el uso de tarjetas inteligentes para el cual es necesario el uso del cifrado del nivel de sockets seguros (SSL), de manera predeterminada Outlook Web Access utiliza SSL por lo que si desea usar la autenticación mediante tarjeta inteligente deberá mantenerlo habilitado o habilitarlo en necesario, además deberá obtener y configurar un certificado de una entidad de certificación de confianza.

Nota: Si desea más información sobre como configurar Outlook Web Access para el uso de una tarjeta inteligente visite el siguiente sitio web: https://technet.microsoft.com/en-us/library/bb691090(v=exchg.80).aspx

3.5. CERTIFICADOS

Cuando se instala Microsoft Exchange Server 2016, se configura por defecto un certificado autofirmado en los servidores de buzones de correo. Este certificado autofirmado se usa para cifrar comunicaciones entre el servidor de acceso de cliente y el servidor de buzones de correo.

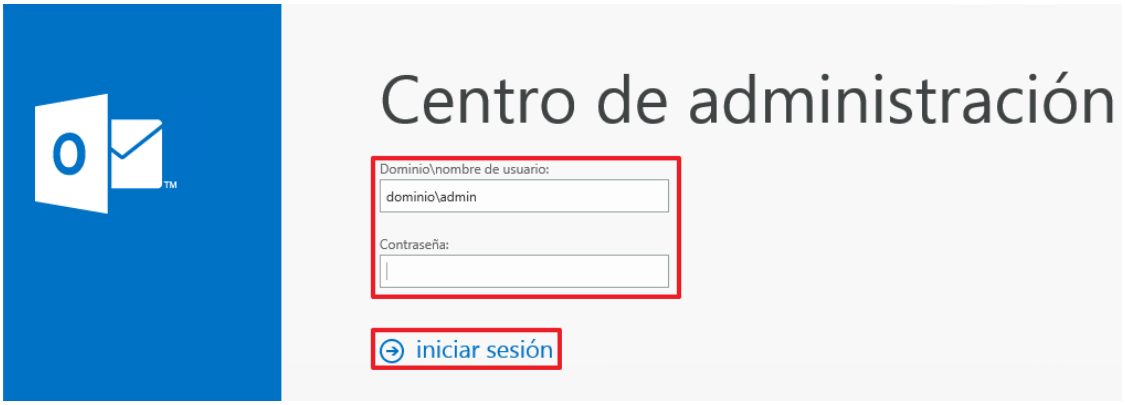
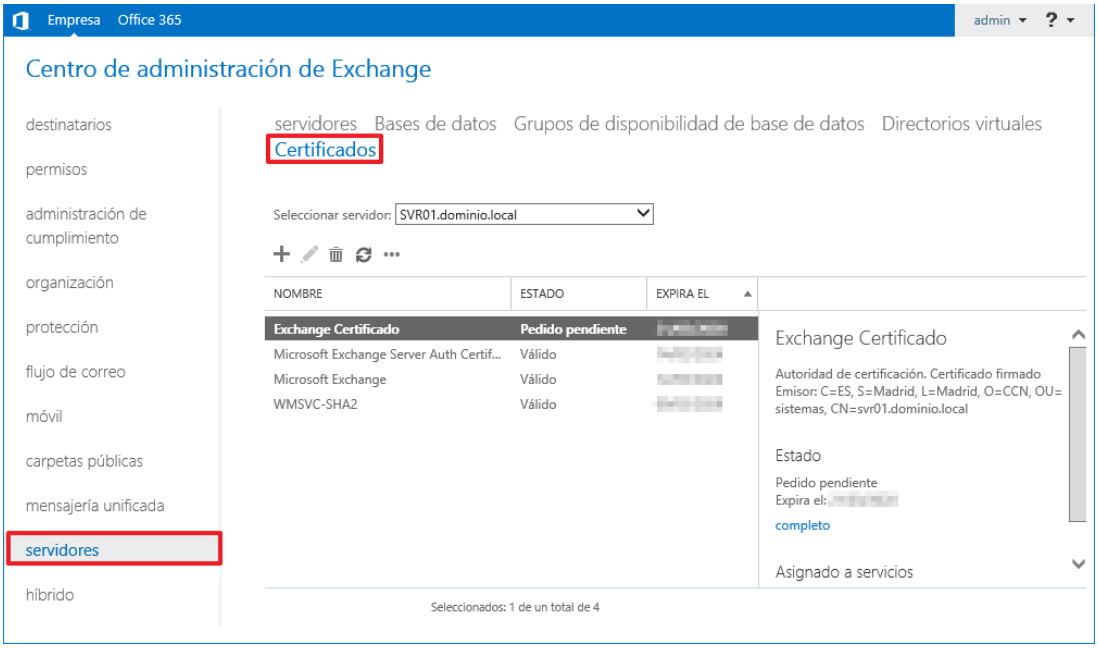
El servidor de acceso de cliente confía en el certificado autofirmado del servidor de buzones de correo automáticamente, así que no es necesario un certificado de terceros en el servidor de buzones de correo. Este certificado autofirmado permitirá que algunos protocolos de cliente usen SSL para sus comunicaciones. Exchange ActiveSync y Outlook Web App, pueden establecer una conexión SSL usando un certificado autofirmado.

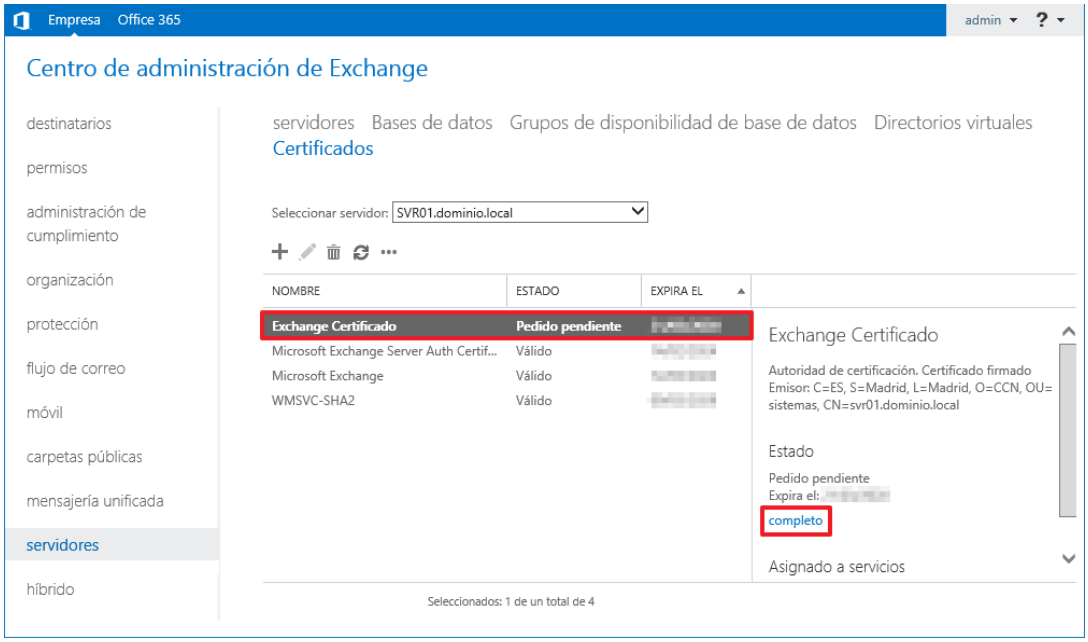
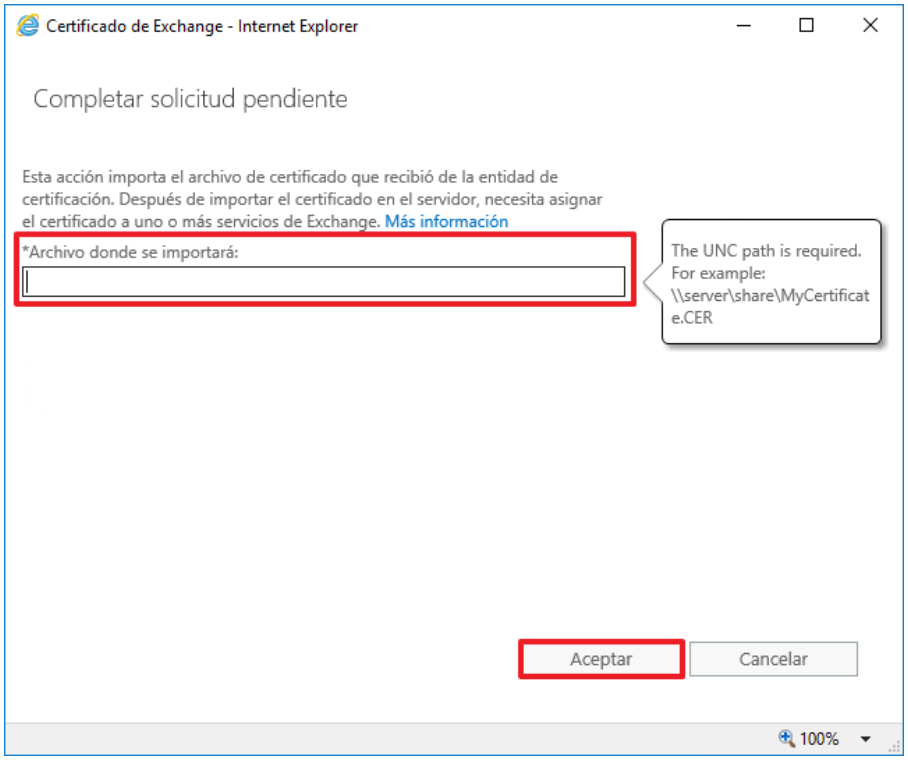
Sin embargo, el certificado autofirmado no es el más recomendable a la hora de implementar mecanismos de seguridad que requieran la confianza de clientes y usuarios ya que es relativamente sencillo suplantar la identidad de un certificado de estas características. Para evitar esto, se requiere la emisión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

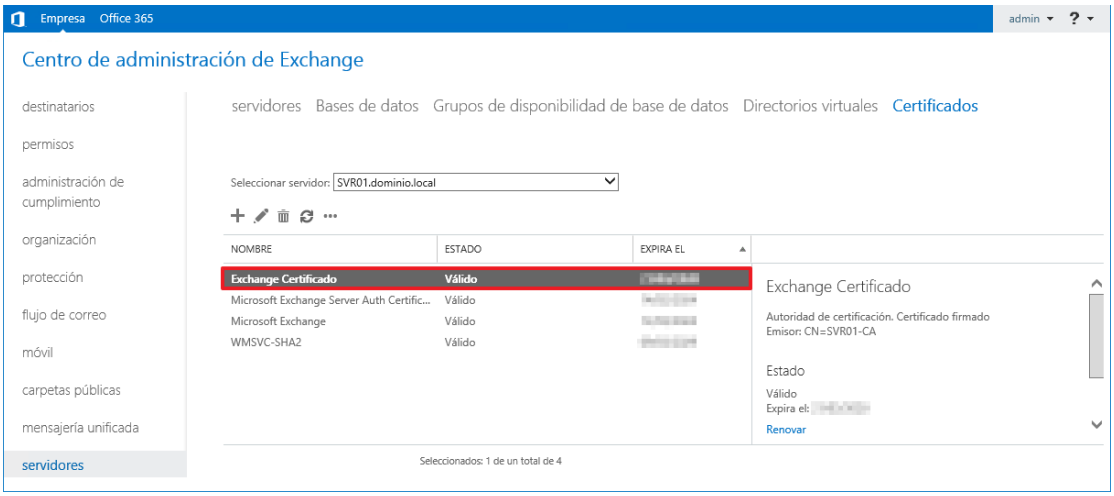
La implementación de certificados puede realizarse bien empleando certificados emitidos por una entidad certificadora que la organización haya implementado o bien por un certificado adquirido a una entidad certificadora de terceros como puede ser la FNMT (Fábrica Nacional de Moneda y Timbre).

A continuación, se muestra un ejemplo de cómo instalar un certificado emitido por una entidad certificadora autorizada, en este paso a paso se da por hecho que ya se ha solicitado un certificado a una entidad de certificación autorizada y se ha obtenido el certificado por lo que se explicara como instalarlo.

Paso	Descripción
94.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
95.	Pulse sobre "Internet Explorer" en la barra de tareas. 
96.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  https://SVR01/ecp Configuración de segurida... **Configuración de seguridad mejorada de Internet Explorer está habilitada** Configuración de seguridad mejorada de Internet Explorer está actualmente habilitada en el servidor. Con ella se configuran una serie de valores de seguridad que definen el modo en que los usuarios exploran sitios web de Internet e intranet. La configuración reduce también la vulnerabilidad del servidor a sitios web que puedan suponer un riego de seguridad. Para obtener un listado completo de los valores de seguridad de esta configuración, consulte Efectos de la configuración de seguridad mejorada de Internet Explorer. Este nivel mejorado de seguridad puede impedir que algunos sitios web se muestren correctamente en Internet Explorer y restringir el acceso a recursos de red, como archivos en recursos compartidos de convención de nomenclatura universal (UNC). Si desea explorar un sitio web que requiera la funcionalidad de Internet Explorer que se ha deshabilitado, agregue el sitio web a las listas de inclusión de las zonas Intranet local y Sitios de confianza. Para obtener más información, consulte Administrar la configuración de seguridad mejorada de Internet Explorer. **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.

Paso	Descripción
97.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
98.	Seleccione en el menú lateral izquierdo la opción "servidores" y a continuación seleccione "Certificados".  **Nota:** En este ejemplo se da por hecho que se ha solicitado previamente un certificado emitido por una entidad certificadora autorizada para este servidor.

Paso	Descripción
99.	Seleccione el certificado el cual solicito previamente, y se encuentra en estado "Pedido pendiente". Pulse en el lateral derecho de la pantalla sobre "completo" para finalizar la instalación del certificado. 
100.	A continuación, seleccione el certificado .cer obtenido y pulse sobre "Aceptar". 

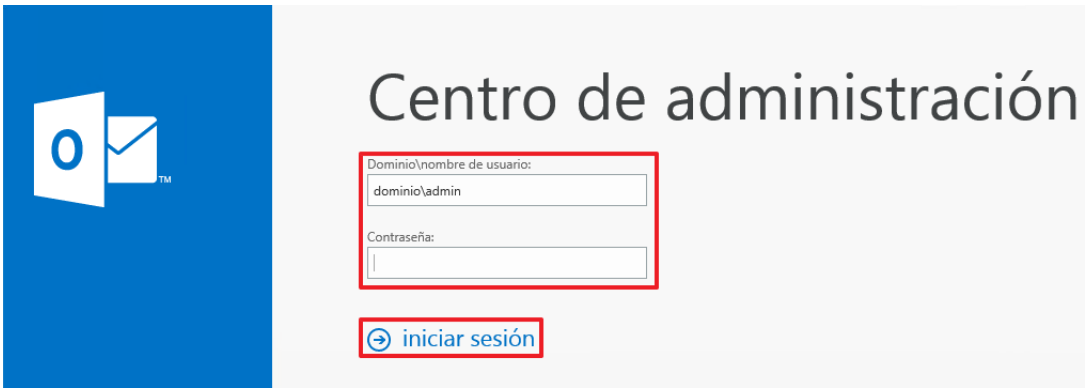
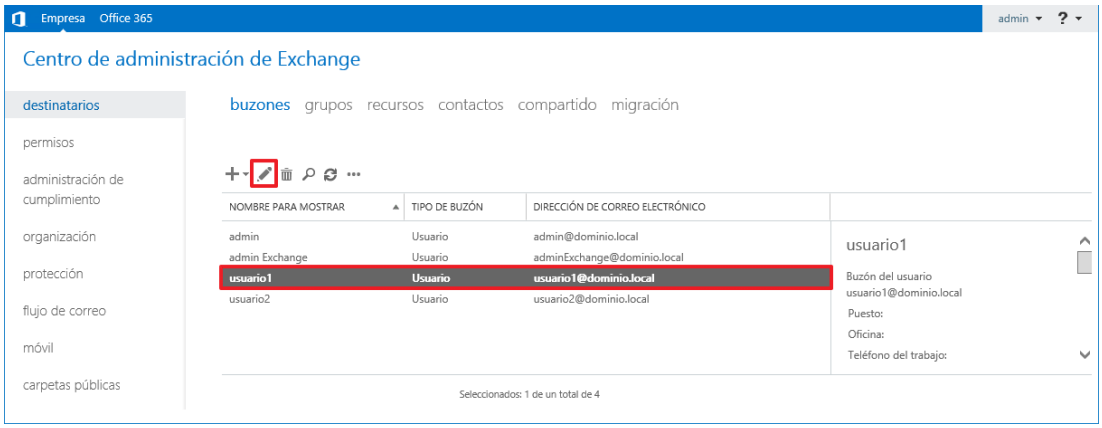
Paso	Descripción
101.	Compruebe que el estado del certificado instalado es válido y está asignado a los servicios que solicitó previamente. 

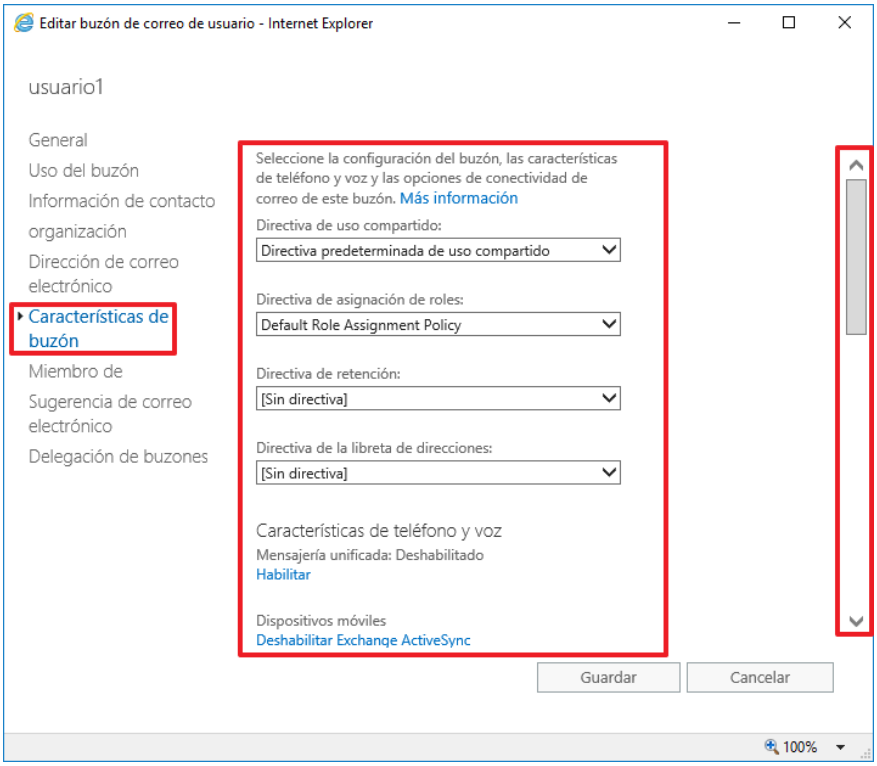
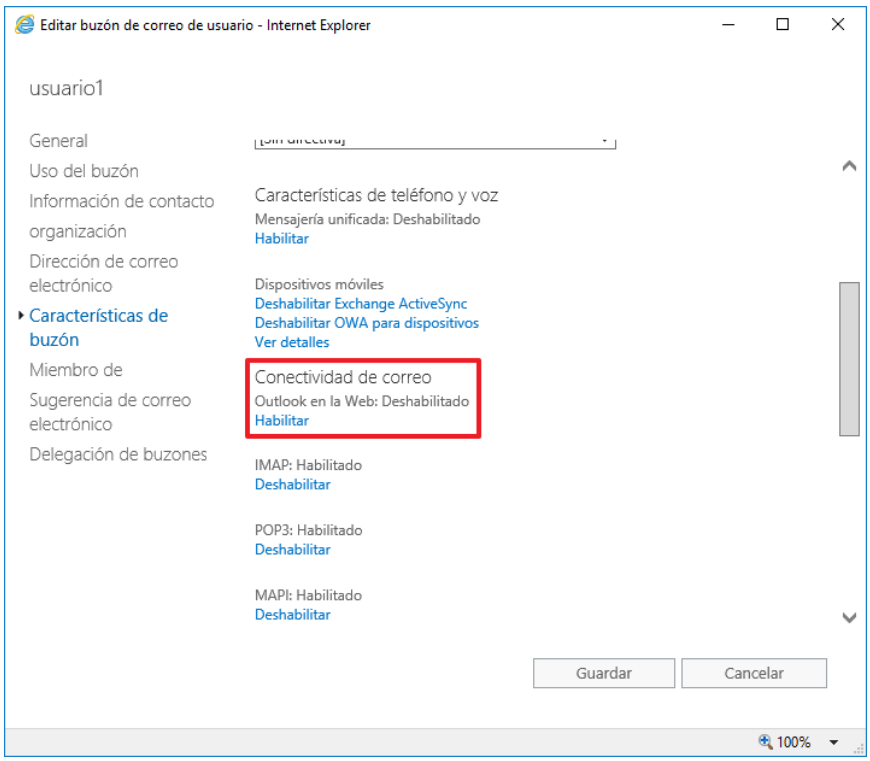
3.6. CONFIGURACIÓN DE SEGURIDAD

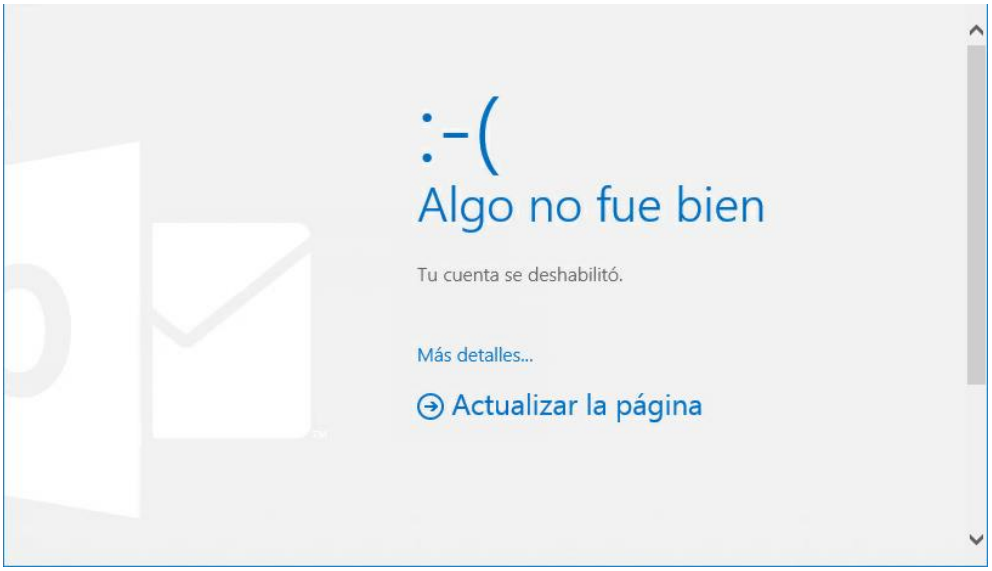
Microsoft Exchange Server 2016 instala POP3 e IMAP por defecto, pero los servicios se encuentran deshabilitados por lo que si es necesario su uso para su organización deberá habilitarlos manualmente.

En esta guía se va a usar el ejemplo de cómo deshabilitar una funcionalidad de Microsoft Exchange Server 2016 como principio de mínima funcionalidad y mínima exposición, deshabilitando la conectividad de correo Outlook Web App para aquellos buzones que no van a hacer uso de esta funcionalidad, limitando con ello, la exposición y aumentando la seguridad de la organización.

Paso	Descripción
102.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
103.	Pulse sobre "Internet Explorer" en la barra de tareas. 

Paso	Descripción
104.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.
105.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
106.	Seleccione el usuario o buzón en el que desea modificar alguna de las funcionalidades editándolo. Para ello seleccione el buzón que desea editar y pulse "Modificar". 

Paso	Descripción
107.	A continuación, Seleccione del menú lateral izquierdo la opción de "Características de buzón" y seleccione la configuración de buzón según las necesidades de su organización. 
108.	Para realizar este ejemplo se ha deshabilitado la conectividad de correo: Outlook Web App, en el "usuario1" creado en los pasos anteriores. 

Paso	Descripción
109.	Para comprobar el funcionamiento, al intentar acceder al buzón usando la funcionalidad de OWA, https://nombre_servidor/owa, devuelve un error indicando que la cuenta esta deshabilitada. 

3.7. TAREAS DE MANTENIMIENTO

El fabricante de Microsoft Exchange Server 2016 publica periódicamente una serie de actualizaciones acumulativas que corrigen nuevas vulnerabilidades detectadas, dichas actualizaciones deben ser instaladas para cumplir con el ENS.

Microsoft Exchange Server 2016 no se actualiza automáticamente por lo que para actualizar el producto deberá descargar manualmente las actualizaciones de la página del fabricante.

Para el cumplimiento del ENS es recomendable realizar todas las tareas de actualización previamente en un entorno de test controlado que refleje el entorno de producción de su organización.

Antes de proceder a realizar una actualización acumulativa de Microsoft Exchange Server 2016, es recomendable realizar un backup previo del estado de los controladores de Active Directory, del rol de Mailbox (backup completo de las bases de datos) y del Client Access (Backup del IIS), además se tendrá que tener en consideración posibles personalizaciones del código por ejemplo de la interfaz gráfica del Outlook Web App el cual deberá ser respaldado para no sufrir pérdidas durante la instalación de la actualización.

Nota: Si desea obtener más información sobre las actualizaciones acumulativas de Microsoft Exchange Server 2016 visite el sitio web: https://technet.microsoft.com/es-es/library/hh135098(v=exchg.150).aspx.

3.8. REGISTRO DE ACTIVIDAD

Con la aplicación del ENS para la categoría media sobre Exchange Server 2016 quedará registrado el uso del sistema para poder detectar y reaccionar a cualquier fallo accidental o deliberado, quedando registrado en el sistema quien realiza la actividad, cuando y sobre qué información con el fin de detectar anomalías o intentos frustrados de acceso a información no autorizada.

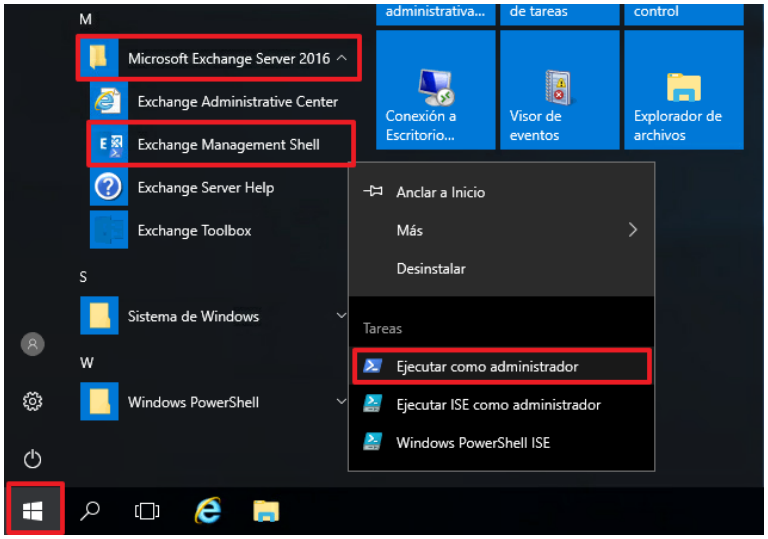
Es recomendable que la ubicación de los registros sea diferente a la del sistema además de tener limitado el acceso únicamente a los usuarios autorizados.

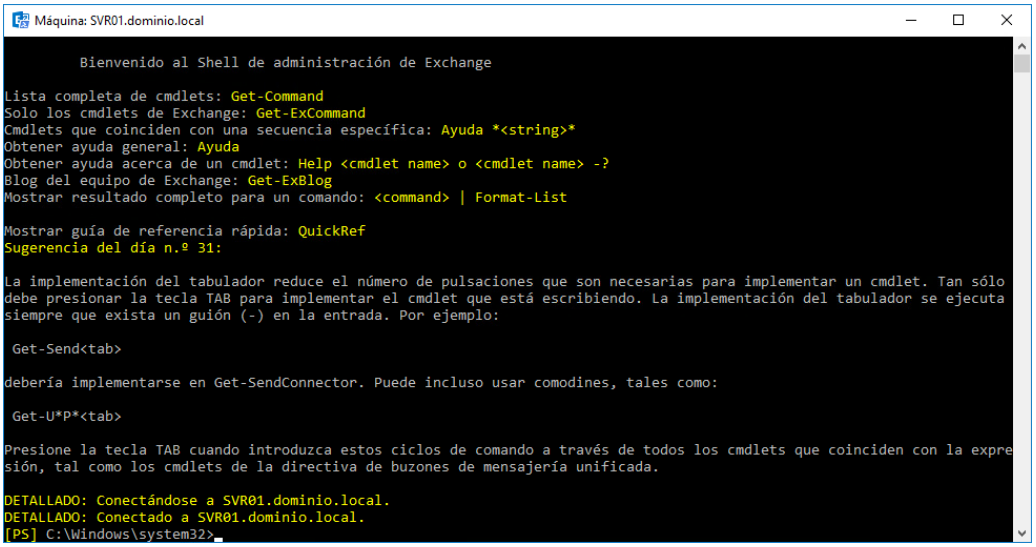
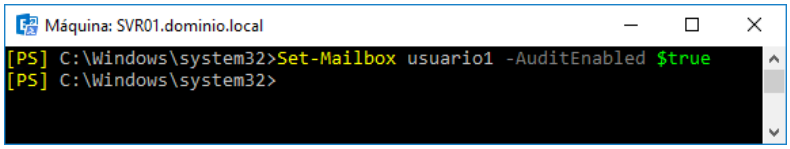
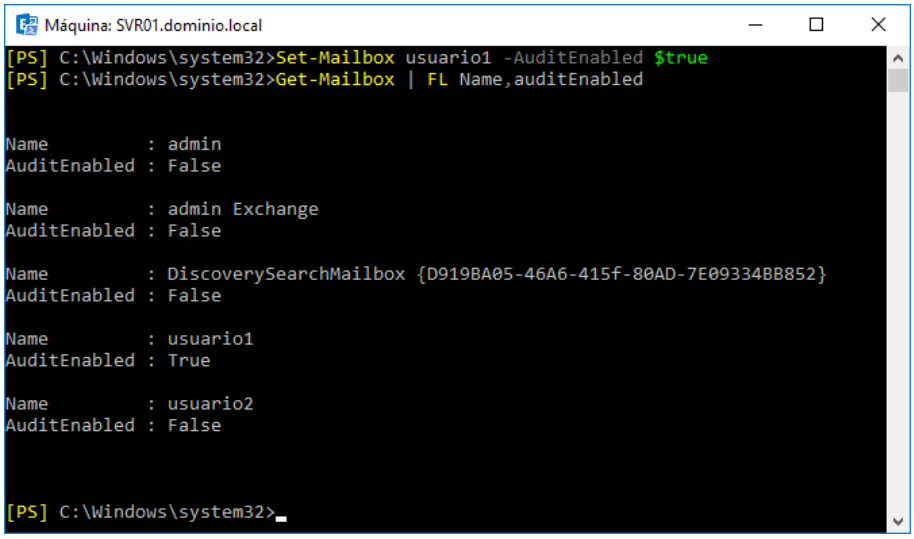
Mediante el registro de auditoría de buzón, se puede registrar el acceso y controlar los inicios de sesión a los buzones de correo por parte de sus propietarios, delegados (incluidos los administradores con permisos de acceso total al buzón) y administradores.

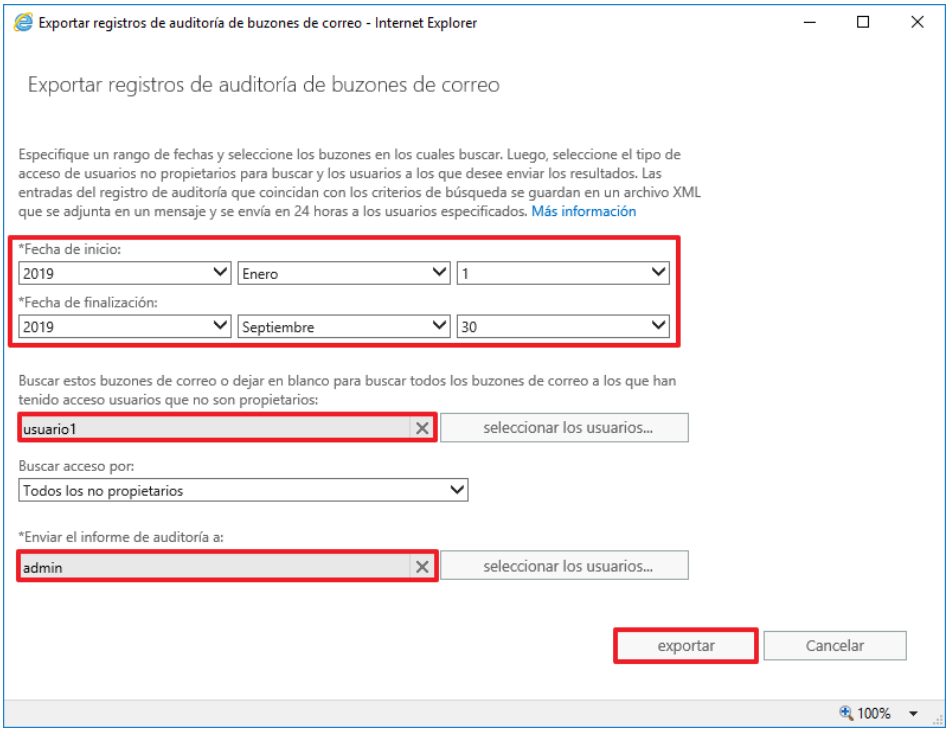
La auditoría de las acciones del propietario del buzón puede generar una gran cantidad de entradas en el registro de auditoría, por lo que se encuentra deshabilitada de forma predeterminada. Se recomienda activar solo la auditoría de algunas acciones específicas necesaria para cumplir con los requisitos comerciales o de seguridad.

Cuando un buzón de correo tiene habilitada la auditoría, Microsoft Exchange Server 2016 guarda la información de accesos al buzón y los elementos del buzón en el registro de auditoría de buzones de correo, siempre que un usuario que no sea el propietario obtenga acceso al buzón de correo.

Cada entrada de registro incluye información acerca de quién tuvo acceso al buzón y en qué momento, así como las acciones realizadas por el usuario que es no propietario y si la acción se realizó correctamente.

Paso	Descripción
110.	Inicie sesión en el servidor miembro donde está instalado Microsoft Exchange Server 2016 con un usuario con permisos de administrador.
111.	Pulse sobre el menú inicio despliegue la carpeta "Microsoft Exchange Server 2016" y pulsando con botón derecho en "Exchange Management Shell" seleccione "Ejecutar como administrador".  **Nota:** El sistema le solicitará elevación de privilegios.

Paso	Descripción
112.	A continuación, se mostrará la siguiente ventana. 
113.	Una vez conectado al Shell, ejecute la siguiente sintaxis. – Set-Mailbox <identity> -AuditEnabled $true  **Nota:** En este ejemplo se habilita la auditoría para el buzón de "usuario1".
114.	Para conocer los buzones donde se encuentra habilitada la auditoria, se puede ejecutar el siguiente cmdlet. – Get-Mailbox | FL Name,auditEnabled 

Paso	Descripción
115.	Es posible exportar los registros de auditoría de buzones desde la consola Web de administración de Exchange desde el menú "administración de cumplimiento" seleccionando la opción "Auditoría", tal y como se ha podido observar en el punto anterior.  **Nota:** Exchange puede tardar hasta 24 horas en generar el informe y enviarlo al destinatario seleccionado
116.	Deberá indicar el intervalo de fechas, los buzones en dónde realizar la búsqueda y el buzón de destino del informe. 

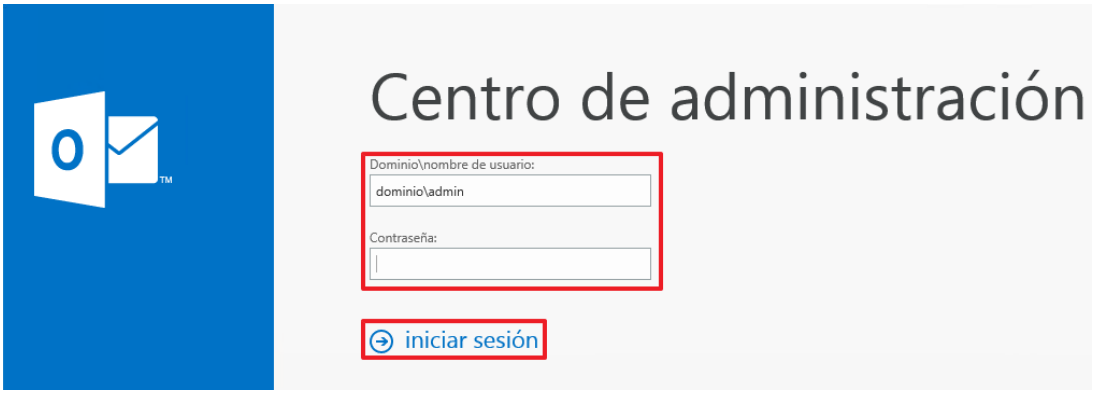
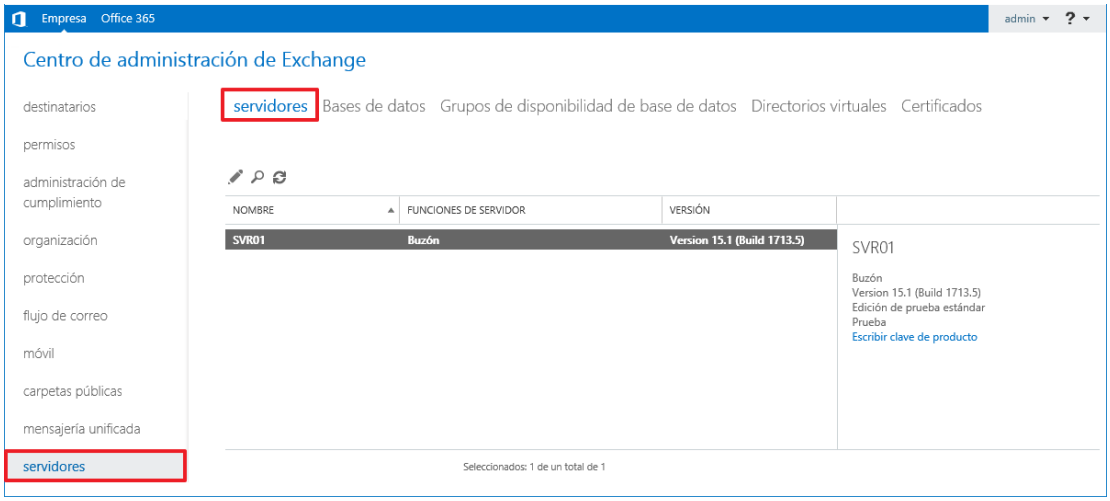
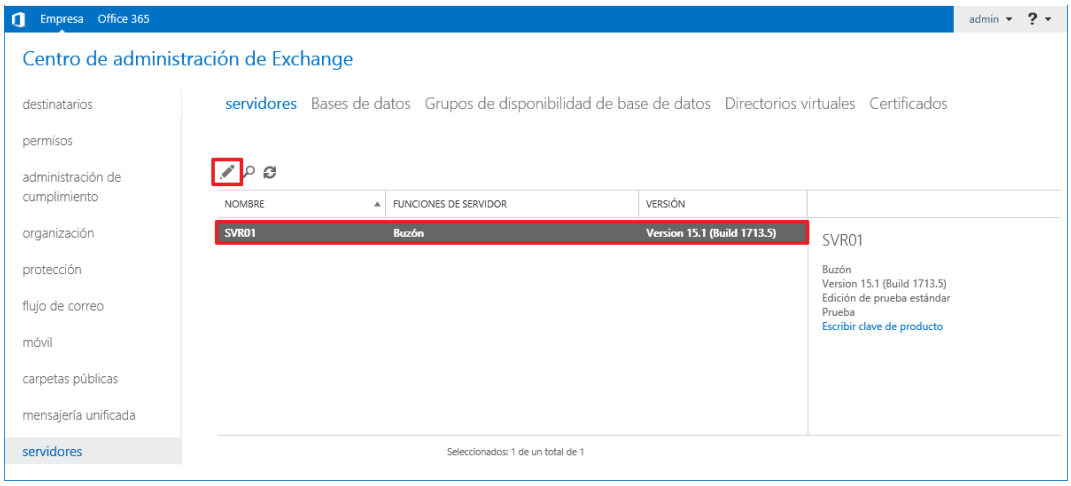
Paso	Descripción
117.	El resultado lo recibirá en su buzón el usuario especificado en la ventana de exportación de registros de auditoría. **Nota:** Debe tener en consideración que, si visualiza el informe desde Outlook Web App, de forma predeterminada se bloquea el acceso a los ficheros ".xml". Si quiere permitir que en Outlook Web App sean accesibles los ficheros ".xml", consulte la información que proporciona Microsoft en el siguiente enlace: https://technet.microsoft.com/es-es/library/jj150552(v=exchg.150).aspx.

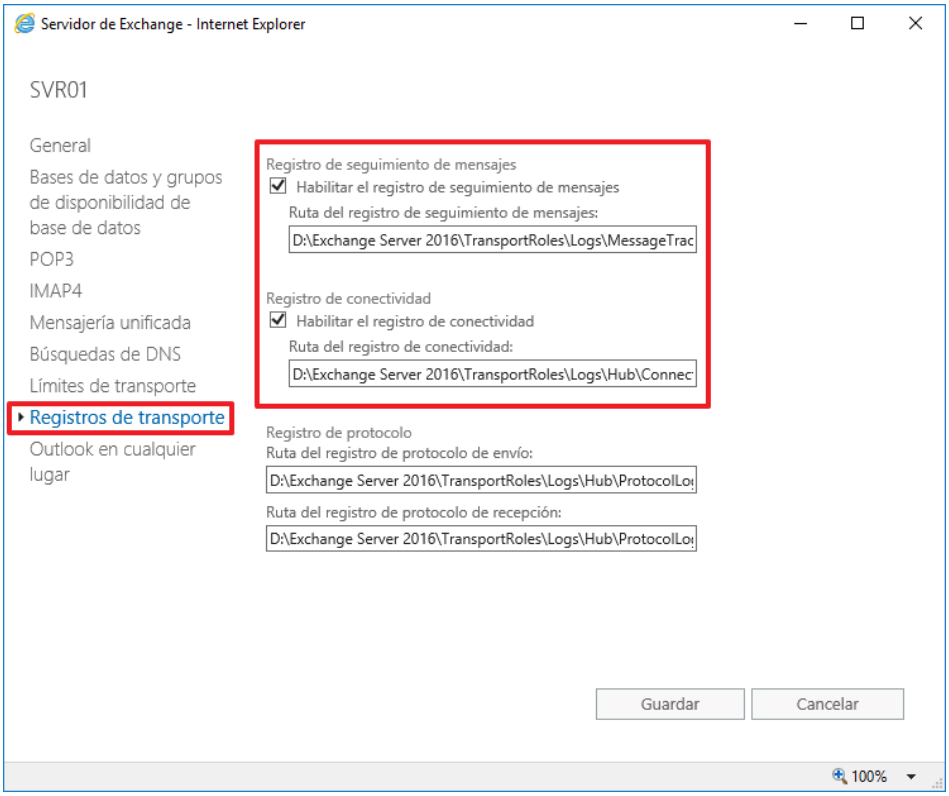
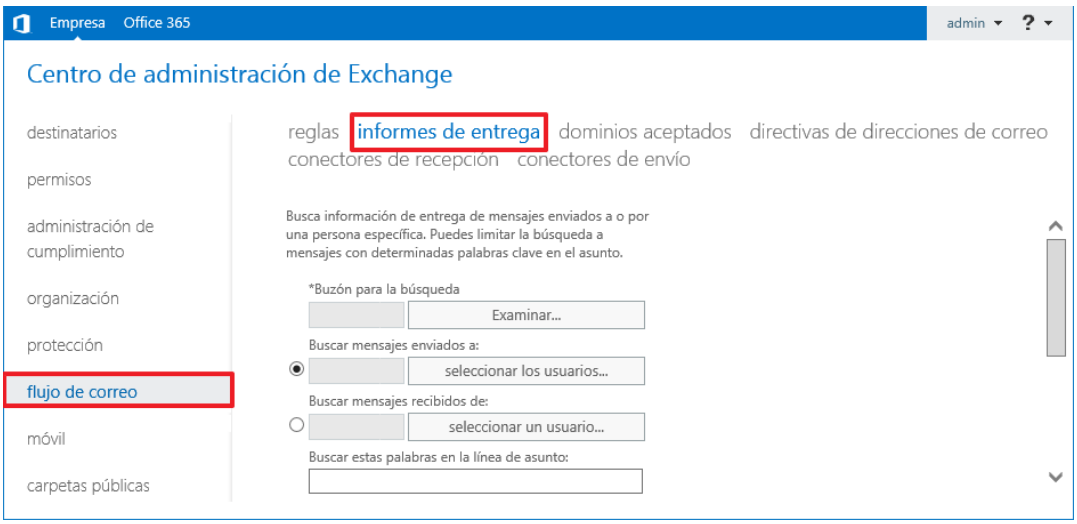
3.9. REGISTRO DE SEGUIMIENTO DE MENSAJES

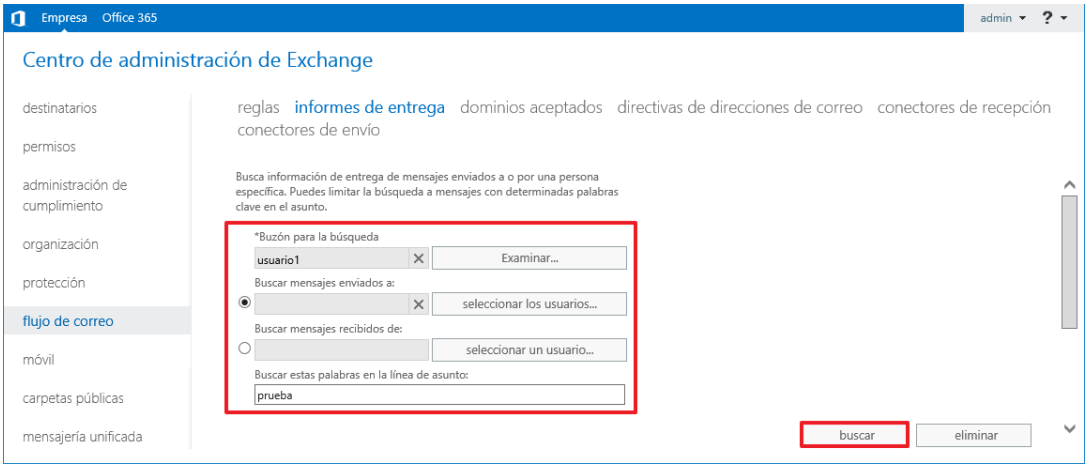
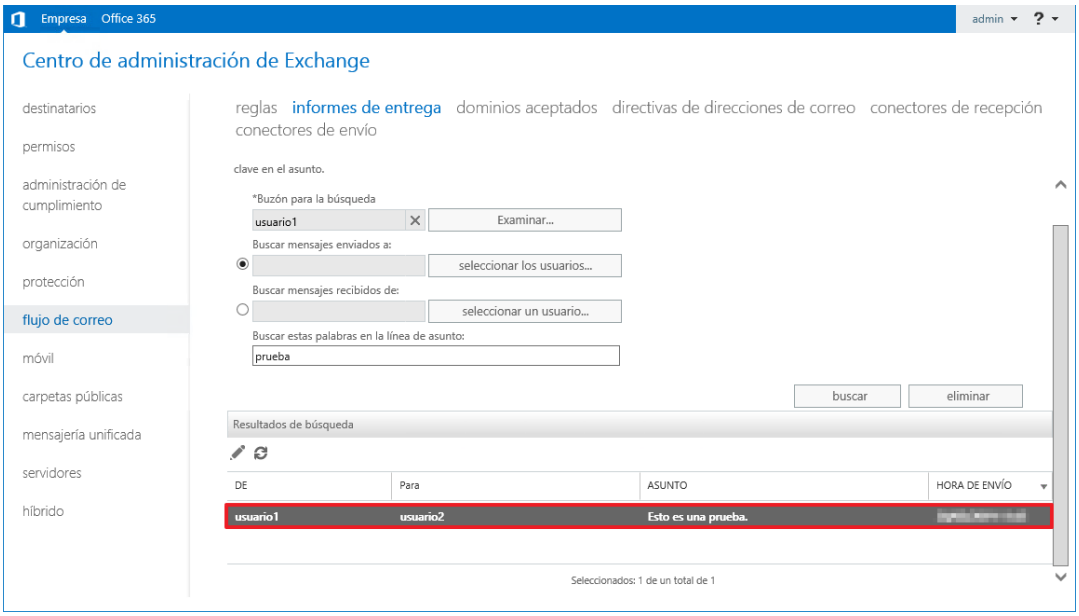
De forma predeterminada, Microsoft Exchange Server 2016 implementa mecanismos de registro para el seguimiento de mensajes y la conectividad de diferentes protocolos. Estos incluyen el envío y recepción de correos, así como la capacidad para analizar el estado de los mismos.

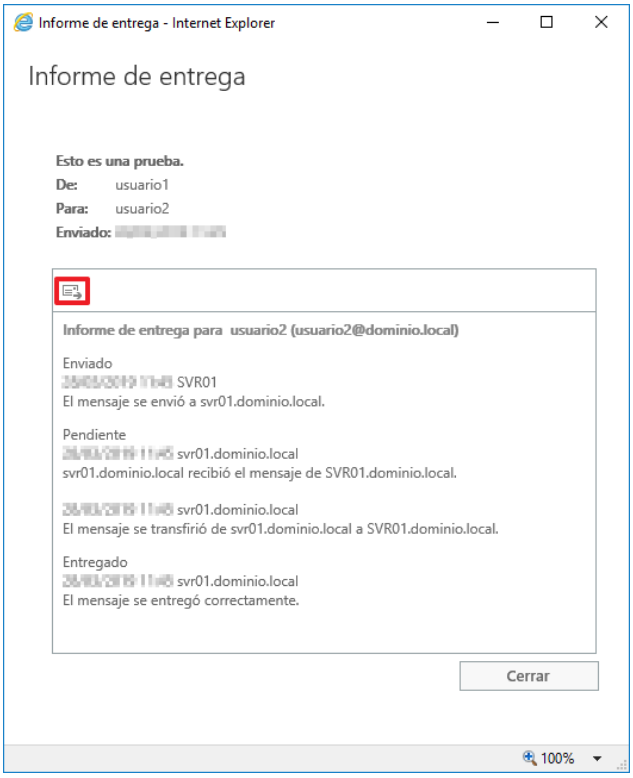
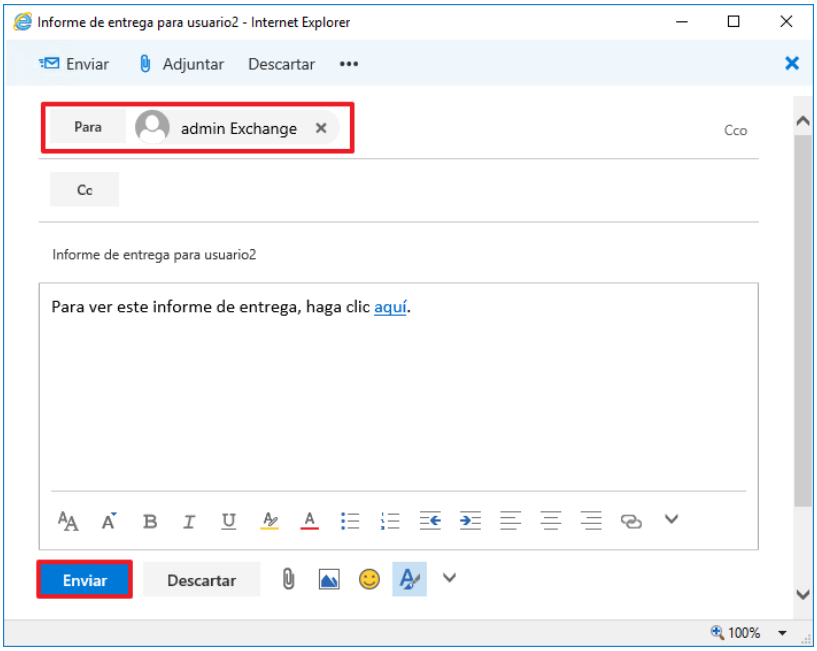
El seguimiento de mensajes se encuentra habilitado, así como los registros de protocolos de comunicaciones, pero podría necesitar modificarlos o bien si han sido desactivados en un momento determinado, poder habilitarlos nuevamente.

Paso	Descripción
118.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
119.	Pulse sobre "Internet Explorer" en la barra de tareas. 
120.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.

Paso	Descripción
121.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
122.	Dentro de la consola de administración de Exchange, seleccione el menú "servidores". A continuación, seleccione "servidores". 
123.	Seleccione el servidor con el rol "Buzón" y a continuación el botón de "Modificar" para dicho servidor. 

Paso	Descripción
124.	En la sección "Registros de transporte" puede modificar la configuración de almacenamiento de cada uno de los registros, así como habilitar y deshabilitar el "Registro de seguimiento de mensajes" y el "Registro de conectividad", tal y como se muestra a continuación. 
125.	Una vez modificadas las propiedades de acuerdo a las necesidades de su organización, pulse el botón "Guardar".
126.	El registro de seguimiento de seguimiento de mensajes lo puede ejecutar desde la propia consola Web de administración de Exchange Server 2016. Para ello, pulse sobre "flujo de correo" y posteriormente en "informes de entrega". 

Paso	Descripción
127.	Puede seleccionar el buzón en el que se desea buscar un mensaje, así como el remitente y/o el destinatario. Con la finalidad de reducir el número de resultados, se pueden escribir palabras clave en la línea de asunto (recuerde que esta funcionalidad sólo permite buscar por el asunto del mensaje y no su contenido).  **Nota:** En este ejemplo se ha utilizado el buzón "Usuario1" y la palabra clave "prueba".
128.	Los resultados se visualizarán en la zona inferior de la pantalla. Pulsando dos veces sobre cada uno de los resultados, se puede obtener un informe de seguimiento del mensaje. 

Paso	Descripción
129.	Así mismo, es posible que necesite enviar el informe de seguimiento al usuario afectado. Para ello pulse sobre el botón de envío y se generará un mensaje con un enlace para que el propio usuario lo pueda visualizar. 
130.	Especifique el destinatario y pulse sobre el botón "Enviar" para enviar el informe de entrega. 
131.	Una vez completadas las búsquedas de seguimiento de mensajes, pulse sobre el botón "Cerrar" y, a continuación, puede cerrar la sesión de la consola Web de administración de Exchange Server 2016.

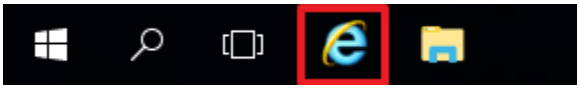
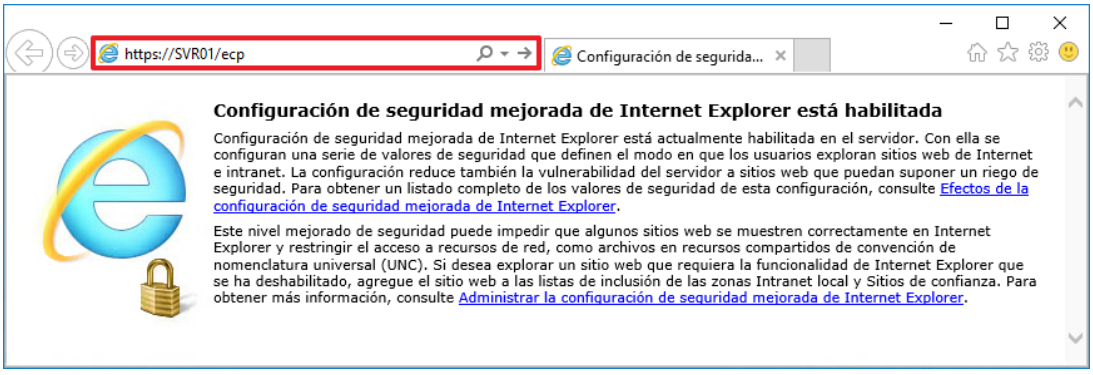
3.10. REGISTRO DE LA GESTIÓN DE INCIDENTES

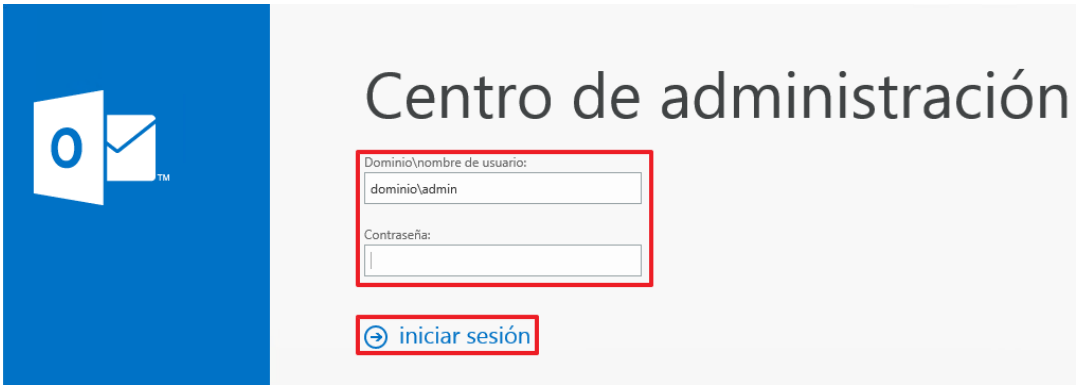
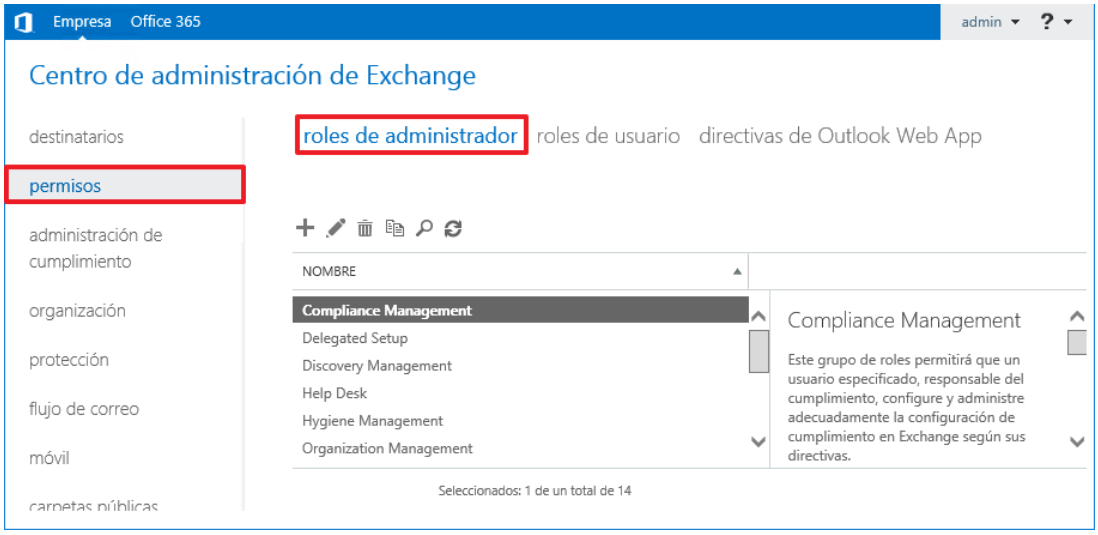
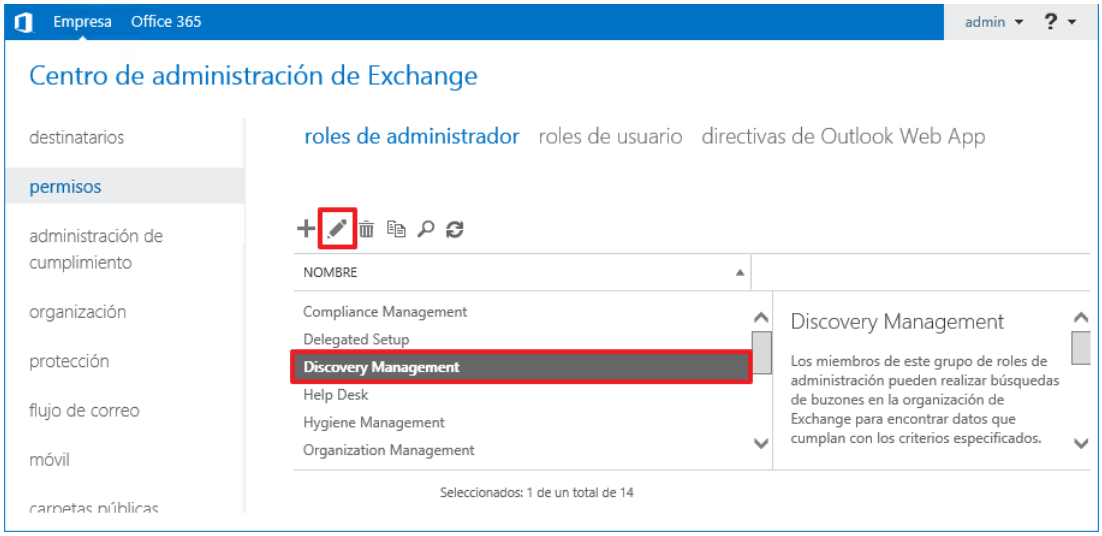
Microsoft Exchange Server 2016 contiene la funcionalidad de retención por juicio, también conocida como retención legal, la cual permite preservar la información almacenada electrónicamente. Cuando se habilita la retención por juicio a un buzón de un usuario, este usuario podrá eliminar elementos del buzón de correo, pero dichos elementos eliminados se retendrán en los servidores. La retención por juicio mantiene los mensajes de correo electrónico, los elementos de calendario, las tareas y otros elementos de buzón de correo, además la retención por juicio protege la versión original de cada elemento del buzón contra una modificación del usuario, por ejemplo, si un usuario cambia las propiedades de los elementos de un buzón y está habilitada la función de retención por juicio, se conserva una copia del elemento antes de que se produzca el cambio.

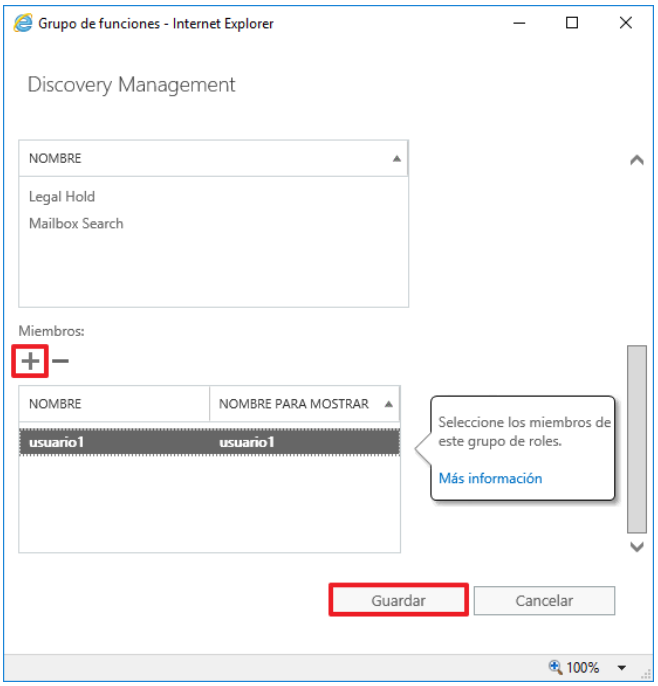
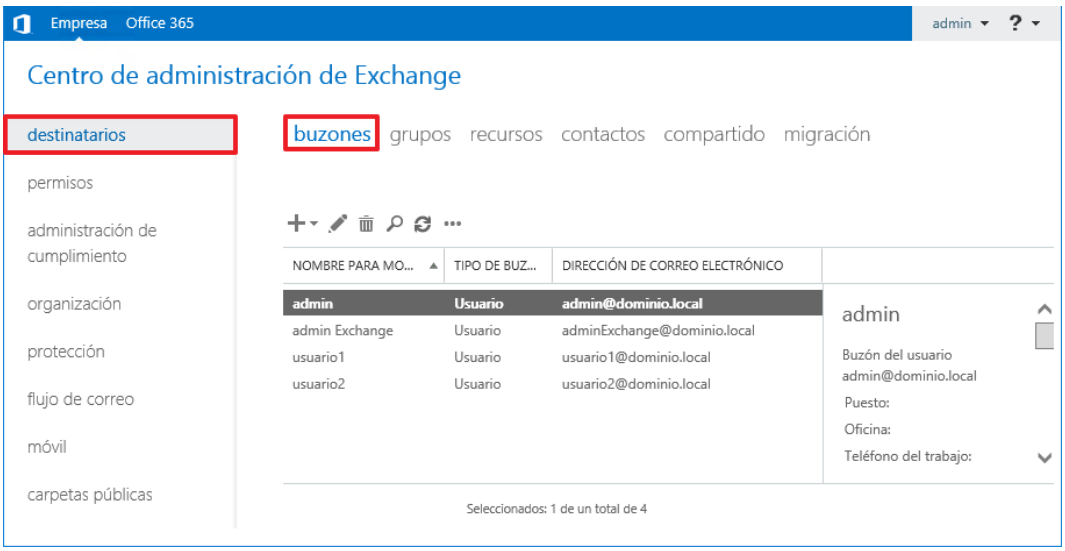
Los usuarios autorizados que han sido agregados al rol de gestión "Discovery Management" o al rol de gestión "Legal Hold", pueden poner buzones de usuarios en el modo de retención legal.

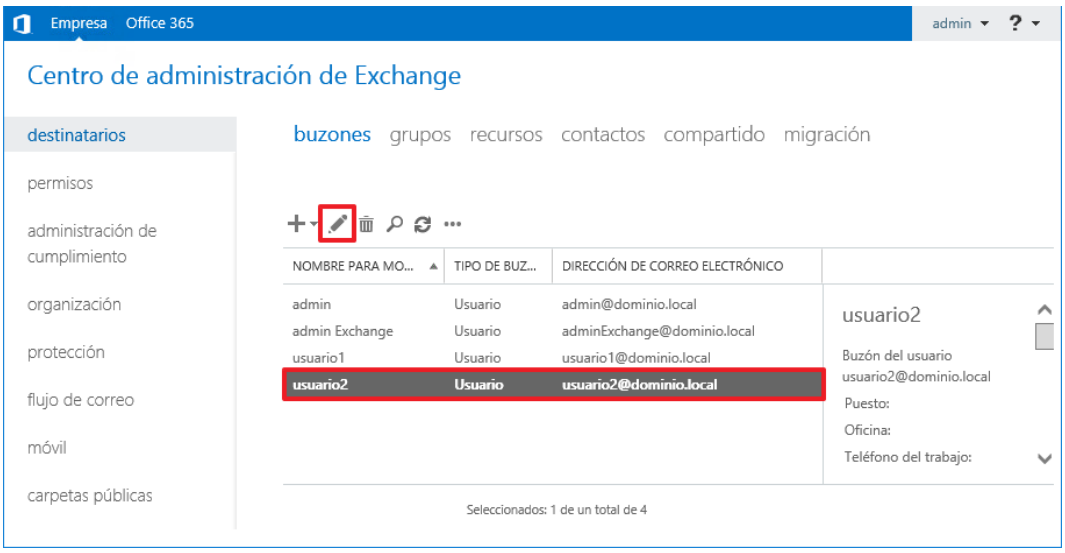
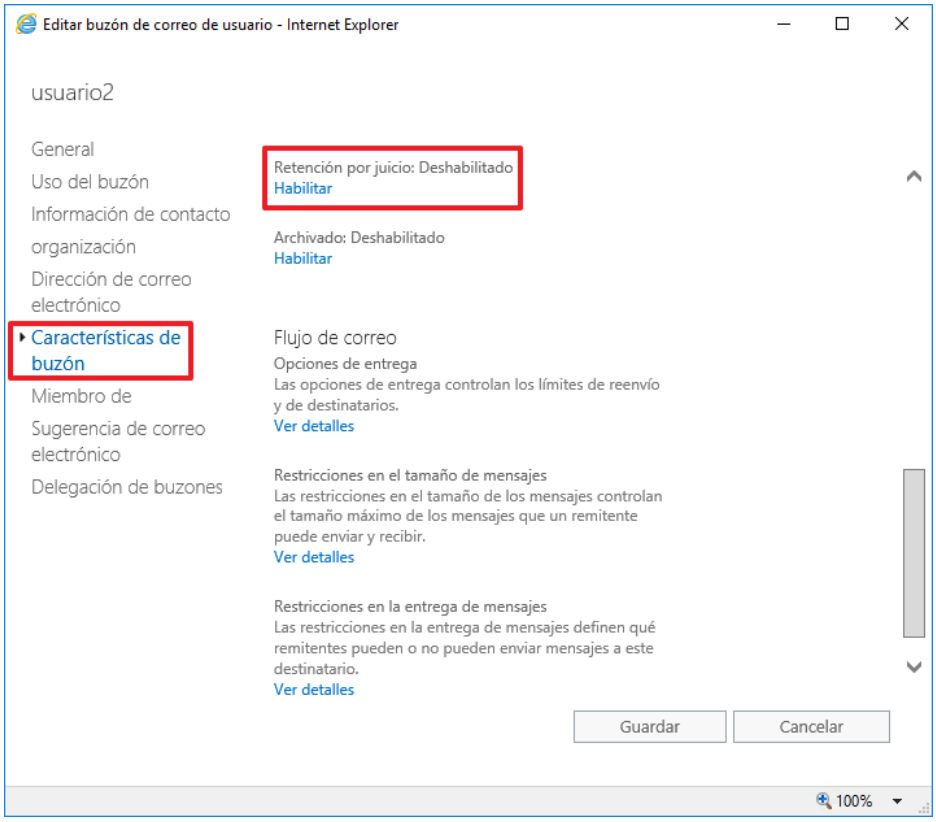
Para habilitar la funcionalidad de retención legal y realizar un análisis de buzones con la opción de retención legal habilitada, el usuario al que se quiera permitir la auditoría, deberá pertenecer al menos al grupo de roles predeterminado "Discovery Management".

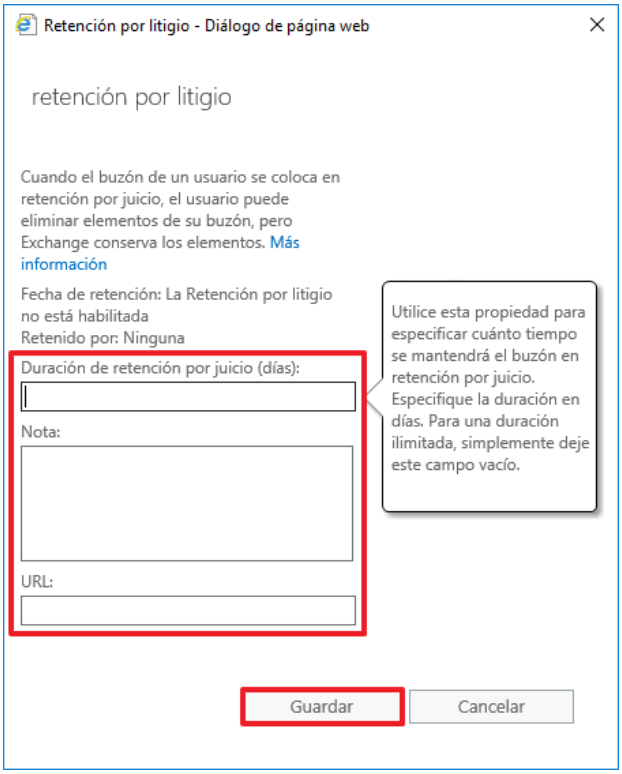
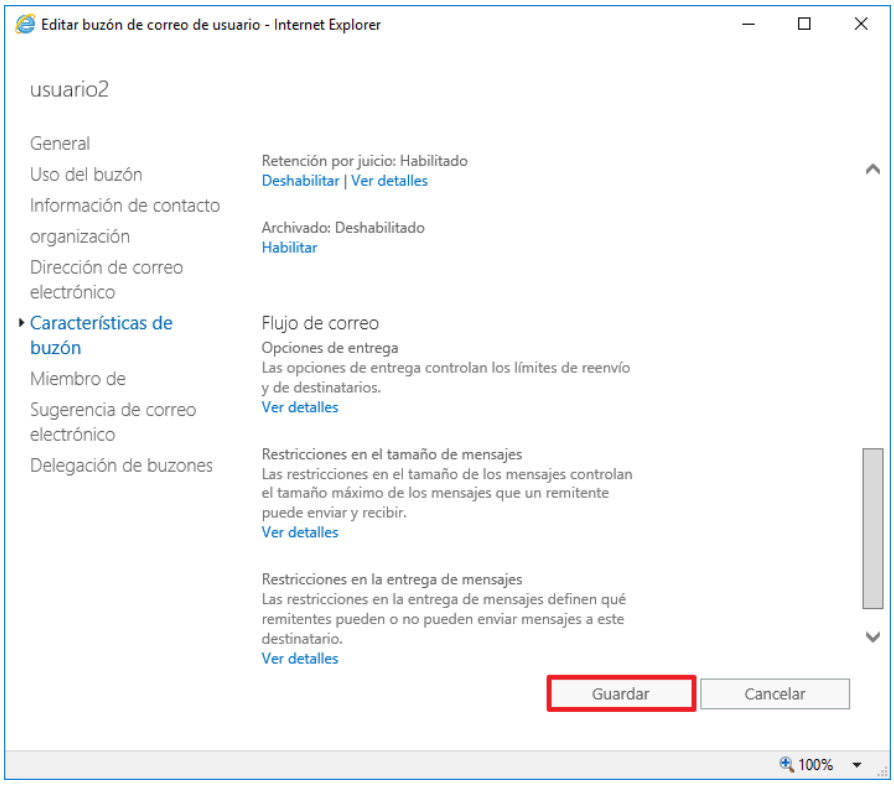
A continuación, se muestra como añadir un usuario al grupo de roles predeterminado "Discovery Management" y como habilitar la retención legal en un buzón de usuario.

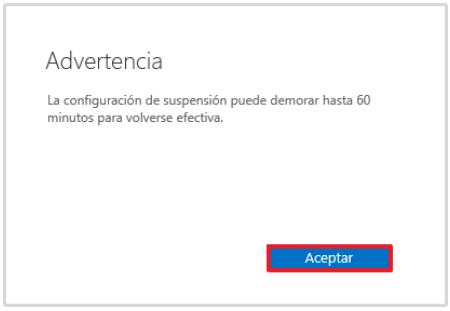
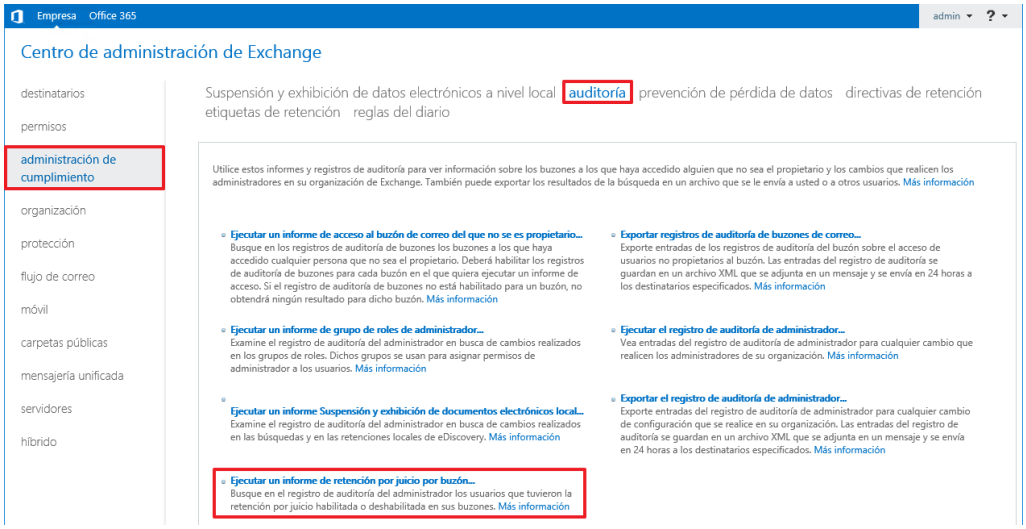
Paso	Descripción
132.	Inicie sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
133.	Pulse sobre "Internet Explorer" en la barra de tareas. 
134.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.

Paso	Descripción
135.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
136.	Seleccione "permisos" y a continuación sitúese en "roles de administrador". 
137.	A continuación, seleccione el grupo de roles "Discovery Management" y pulse "Editar". 

Paso	Descripción
138.	En la sección "Miembros", pulse sobre el botón "+" para agregar las cuentas de los usuarios a los cuales se les quiere otorgar este grupo de roles, para finalizar pulse sobre "Guardar".  **Nota:** En este ejemplo se agrega la cuenta DOMINIO\usuario1 creada previamente, debe adaptar estos pasos a su organización. Además, cabe señalar que los administradores de la organización Exchange, de forma predeterminada no disponen de los permisos para realizar búsquedas en los buzones de tipo suspensión y exhibición de datos electrónicos, aunque sí disponen del permiso para establecer un buzón en modo de retención legal.
139.	A continuación, para habilitar la retención por juicio en un buzón de usuario, diríjase a la sección **"destinatarios → buzones"**. 

Paso	Descripción
140.	Seleccione el buzón de usuario en el cual desea habilitar la retención por juicio y pulse sobre "Modificar".  **Nota:** En este ejemplo se activará la retención por juicio al "usuario2".
141.	En la sección "Características de buzón", pulse sobre el botón "Habilitar" en "Retención por juicio" para activar la retención por juicio sobre el buzón de usuario previamente seleccionado. 

Paso	Descripción
142.	A continuación, complete la siguiente ventana adecuándola a las necesidades de su organización y pulse sobre "Guardar". 
143.	Una vez finalizada la configuración pulse sobre "Guardar" para cerrar la ventana. 

Paso	Descripción
144.	Pulse "Aceptar" en la advertencia. 
145.	Una vez habilitada la retención legal en los buzones correspondientes, es posible obtener un informe sobre los elementos que han sido modificados o eliminados desde el menú **"Administración del cumplimiento → Auditoría → Ejecutar un informe de retención por juicio de buzón"** en la consola Web de administración de Exchange Server 2016. 

3.11. PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD

Uno de los cambios más significativos desde Exchange 2013, es que RPC ya no es un protocolo de acceso directo compatible. Esto significa que la conectividad de Outlook en su totalidad debe realizarse a través del servidor de acceso de cliente mediante RPC sobre HTTP (también conocido como Outlook Anywhere).

El beneficio de este cambio es que no hay necesidad de tener el servicio de acceso de clientes de RPC en el servidor acceso de clientes. Esto ocasiona la reducción de dos espacios de nombres que habitualmente se necesitarían para una solución de resistencia ante fallos a nivel de sitios. Asimismo, ya no hay requerimientos para suministrar afinidad para el servicio de acceso de clientes de RPC.

Junto a esto, Exchange Server 2016 incorpora un protocolo de comunicación con los clientes Outlook denominado MAPI sobre HTTP (no confundir con RPC sobre HTTP o Outlook Anywhere).

MAPI sobre HTTP supone un avance importante en la simplificación de las comunicaciones de los clientes Outlook y el soporte de nuevos mecanismos de autenticación modernos como federación de identidades, autenticación de doble factor u otros.

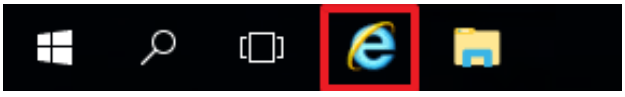
MAPI sobre HTTP traslada la capa de transporte al modelo HTTP para mejorar la confiabilidad y la estabilidad de las conexiones de Outlook y Exchange. Esto permite un mayor nivel de visibilidad de los errores de transporte y una capacidad de recuperación mayor. Entre la funcionalidad adicional se incluye compatibilidad para una función de pausa y reanudación explícitas. Esto permite a los clientes compatibles cambiar de red o reactivarse después de la hibernación, manteniendo el mismo contexto de servidor.

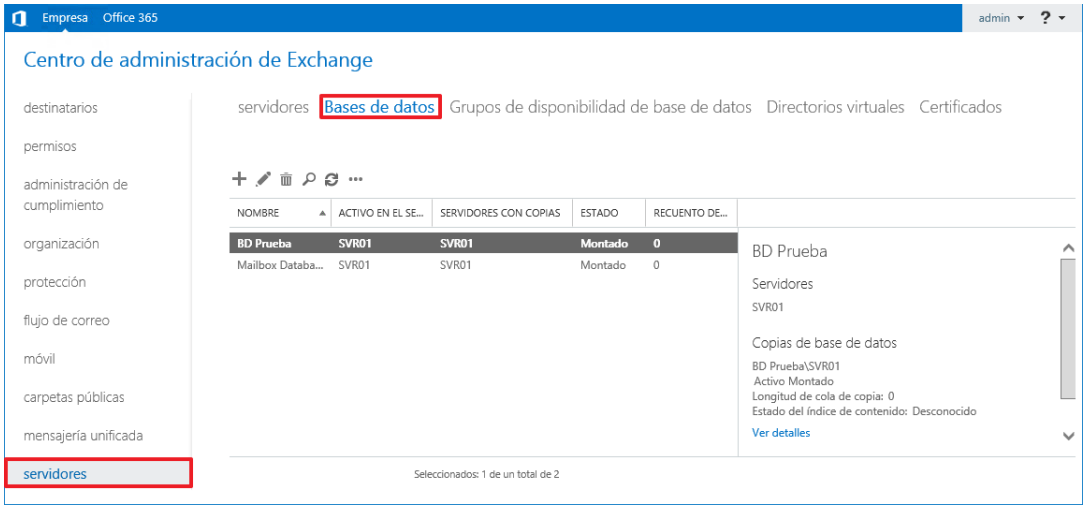
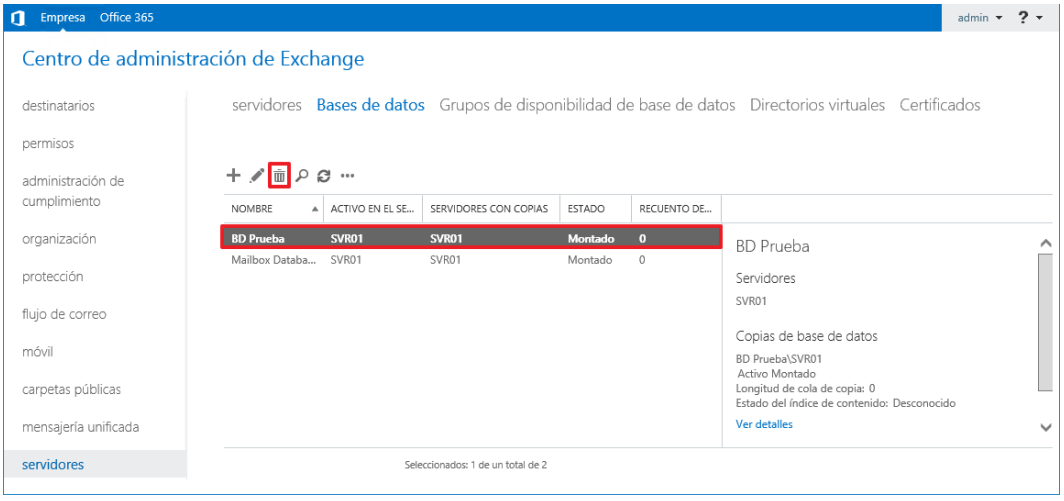
Microsoft Exchange Server 2016 incorpora estas características por defecto desde su instalación, por lo que, si no se desea degradar la seguridad es recomendable no deshabilitar el uso de estos protocolos.

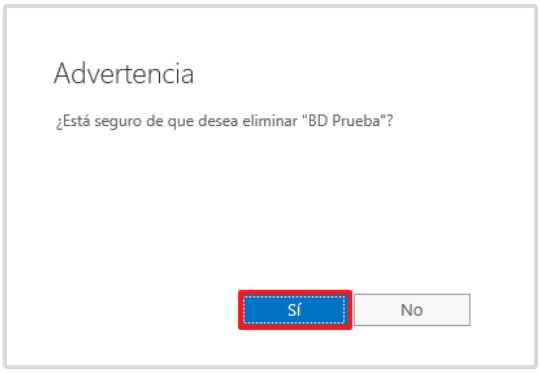
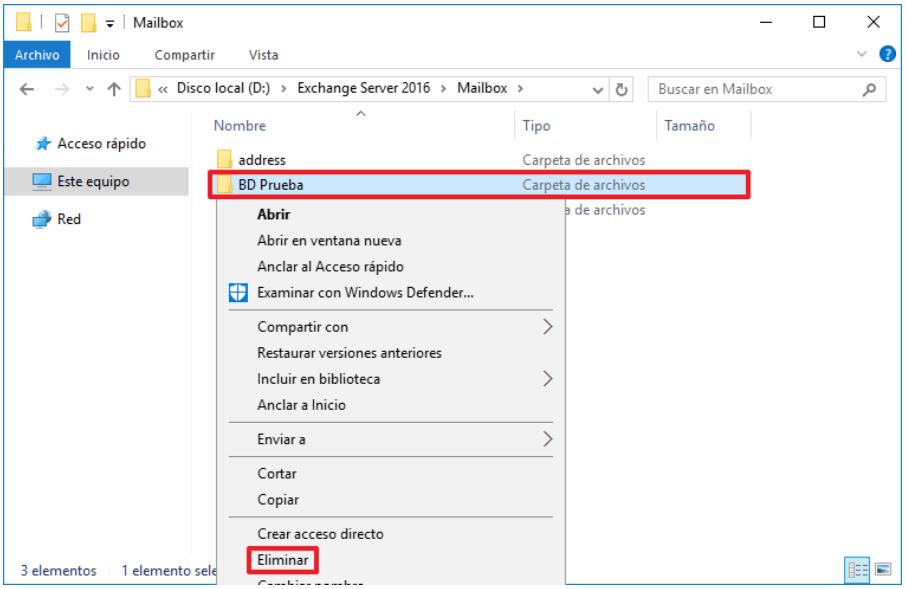
3.12. BORRADO SEGURO DE BASES DE DATOS

En Exchange Server 2016 edición Enterprise se pueden crear hasta 100 bases de datos por cada servidor de buzones, pudiendo alojar miles de buzones de usuarios en cada una de esas bases de datos. No existe un límite impuesto sobre el tamaño de las bases de datos y los buzones en Exchange Server 2016, aunque se recomienda que las bases de datos de buzones no superen los 200 GB para entornos no agrupados y de 2 TB para servidores de buzones en grupos de disponibilidad (DAG) con replicación habilitada.

A continuación, se detalla como eliminar una base de datos de buzones del servidor.

Paso	Descripción
146.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
147.	Pulse sobre "Internet Explorer" en la barra de tareas. 
148.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.

Paso	Descripción
149.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
150.	A continuación, diríjase a **"servidores → Bases de datos"**. 
151.	Seleccione la base de datos que desea eliminar y pulse sobre "Borrar".  **Nota:** Si existen buzones alojados en la base de datos que desea eliminar debería previamente mover los buzones a otra base de datos para que el sistema permita eliminar la base de datos. En este ejemplo se elimina la base de datos "BD Prueba".

Paso	Descripción
152.	Asegúrese que es correcta la base de datos que desea eliminar, y pulse "sí". 
153.	A continuación, le aparecerá una advertencia indicando que debe dirigirse a la ubicación física donde tenía alojada la base de datos y deberá eliminarla manualmente. Pulse "Aceptar" para cerrar la advertencia. 
154.	Diríjase a la ubicación de la base de datos, seleccione la base de datos que acaba de eliminar de la consola de administración de Exchange 2016 y elimine manualmente la carpeta de la base de datos.  **Nota:** El sistema le solicitará elevación de privilegios para acceder a la ruta donde se alojan las bases de datos.

3.13. PROTECCIÓN DE DATOS Y RECUPERACIÓN DE ELEMENTOS ELIMINADOS

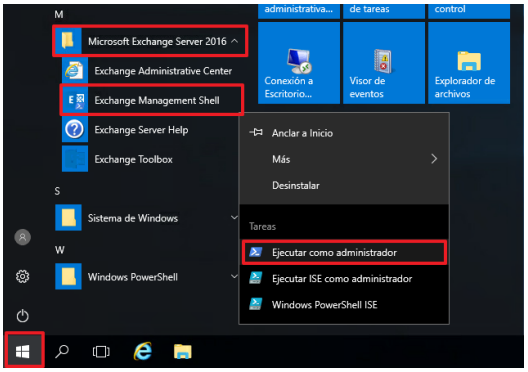
Microsoft para Exchange Server 2016 usa un concepto conocido como Exchange Native Data Protection, el cual se basa en características integradas de Exchange para proteger los datos de su buzón de correo sin tener que usar copias de seguridad (aunque puede seguir utilizando dichas características para crear copias de seguridad). Exchange 2016 incluye varias características nuevas y cambios generales que, una vez implementados y configurados correctamente, ofrecen una protección de datos nativa que elimina la necesidad de realizar copias de datos tradicionales.

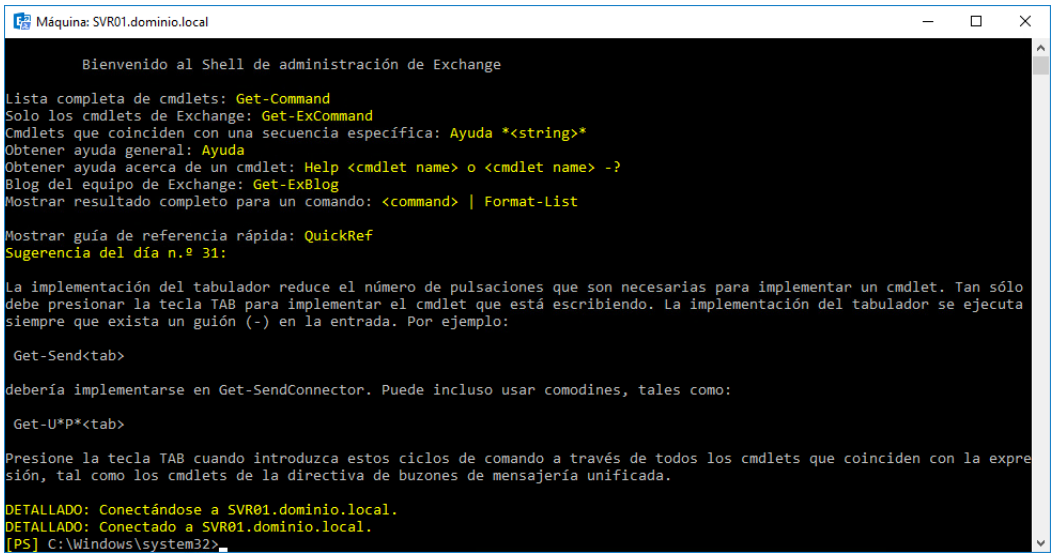
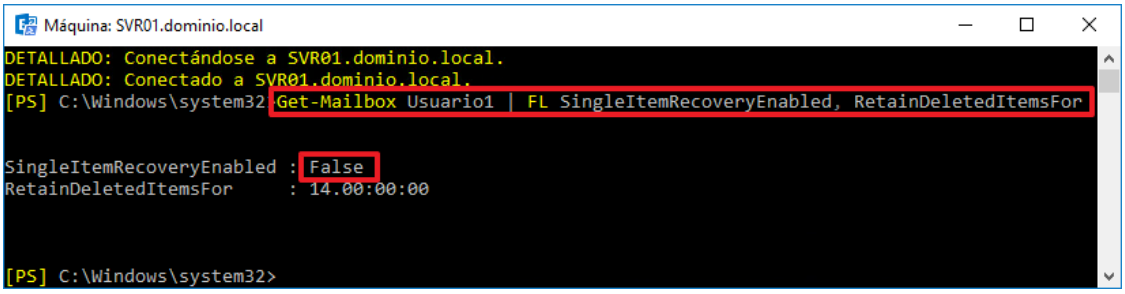
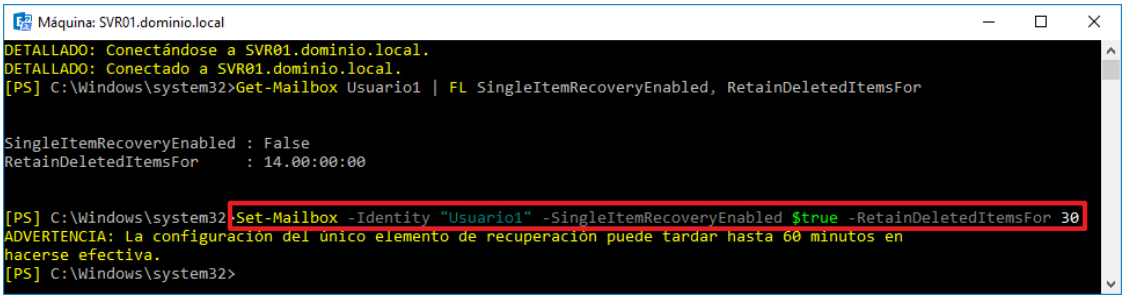
Exchange 2016 también implementa los grupos de disponibilidad de bases de datos (DAG). Un grupo de disponibilidad de base de datos (DAG) es el componente básico del marco de alta disponibilidad y resistencia de sitios del servidor de buzones que ofrece Microsoft Exchange Server 2016. Un DAG es un límite para la replicación de bases de datos de buzones, los cambios de bases de datos y de servidores, y las conmutaciones por error, así como para un componente interno denominado Active Manager.

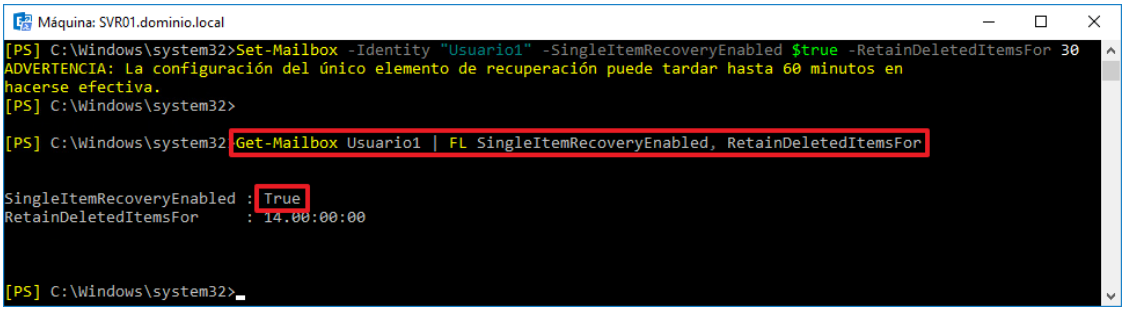
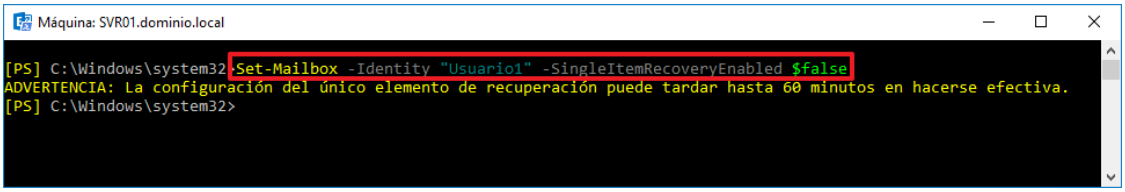
Cualquier servidor en un DAG puede hospedar una copia de una base de datos de buzones de correo de cualquier otro servidor en el DAG. Cuando se agrega un servidor a un DAG funciona con los otros servidores del DAG para proporcionar recuperación automática de errores que afectan a las bases de datos de buzones, como un error de disco, de servidor o de red.

Además, Microsoft Exchange Server 2016, también ofrece la recuperación de un elemento único la cual se deshabilita cuando se crea un buzón. Si la recuperación de un elemento único está habilitada, los mensajes que el usuario elimina (purga) permanentemente se conservan en la carpeta Elementos recuperables del buzón hasta que expira el período de retención de elementos eliminados. Esto permite al administrador recuperar los mensajes purgados por el usuario antes de que expire el período de retención de elementos eliminados.

A continuación, se muestra como habilitar la recuperación de un elemento único el cual viene deshabilitado por defecto.

Paso	Descripción
155.	Inicie sesión en el servidor miembro donde está instalado Microsoft Exchange Server 2016 con un usuario con permisos de administrador.
156.	Pulse sobre el menú inicio despliegue la carpeta "Microsoft Exchange Server 2016" y pulsando con botón derecho en "Exchange Management Shell" seleccione "Ejecutar como administrador".  **Nota:** El sistema le solicitará elevación de privilegios.

Paso	Descripción
157.	A continuación, se mostrará la siguiente ventana. 
158.	A continuación, si desea comprobar si está habilitada la recuperación ejecute el comando y compruebe que el estado es “False”. – “Get-Mailbox <Nombre_buzon> | FL SingleItemRecoveryEnabled, RetainDeletedItemsFor” Sustituya “<Nombre_buzon>” por el nombre de buzón que desea comprobar. 
159.	A continuación, para habilitar la recuperación de elementos eliminados ejecute el siguiente comando. – “Set-Mailbox -Identity "Usuario1" -SingleItemRecoveryEnabled $true -RetainDeletedItemsFor 30” Además, se establecerá que el tiempo de conservación de los correos será de 30 días. 

Paso	Descripción
160.	Compruebe que ha habilitado correctamente la recuperación de elementos eliminados. Ejecute nuevamente el siguiente comando. – "Get-Mailbox <Nombre_buzon> | FL SingleItemRecoveryEnabled, RetainDeletedItemsFor" Compruebe que el estado es "True". 
161.	En caso de que desee deshabilitar la recuperación de elementos eliminados deberá ejecutar el comando. – "Set-Mailbox -Identity "Nombre_Usuario" -SingleItemRecoveryEnabled $false"  **Nota:** Si desea más información acerca de la recuperación de elementos eliminados en Exchange Server 2016 visite el sitio web: https://technet.microsoft.com/es-es/library/ee633460(v=exchg.150).aspx

3.14. PROTECCIÓN DE SERVICIOS

Exchange Server 2016 utiliza IIS por lo que todos los sistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que le competen como:

a) Ataques directos, tales como accesos no autorizados sobre cualquiera de los elementos que conforman el entorno.

b) Ataques indirectos, dónde cualquiera de los elementos es empleado como herramienta en el ataque.

c) Ataques de denegación de servicio (DoS). Las arquitecturas Web están basadas en tecnologías TCP/IP y por tanto son vulnerables a los ataques de DoS comunes en TCP/IP. Es necesario disponer de contramedidas técnicas y procedimientos de actuación frente a este tipo de ataques.

Para una mayor seguridad sobre Exchange Server 2016 se han de configurar los filtros de solicitudes los cuales permiten controlar las conexiones entre servidor y cliente, restringiendo el comportamiento de protocolos y contenidos.

Se considera una buena práctica de seguridad realizar una configuración básica para el servidor según los usos, situación, contenidos a servir, etc. que se le prevén y luego afinar aún más en cada uno de los sitios que se generen.

El filtro de solicitudes es un módulo, o servicio de rol, de IIS instalable (por medio de AppCMD.exe, Administrador del servidor, Powershell, etc.) de forma individual y configurable por cualquiera de los medios habituales (Administrador de Internet Information Services (IIS), AppCMD.exe, etc.).

En el apartado "2 PREPARACIÓN DEL IIS 10" se aplica seguridad sobre URLfiltering para Microsoft Exchange Server 2016.

ANEXO A.3.2. LISTA DE COMPROBACIÓN

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía "ANEXO A.3.1PASO A PASO PARA LA IMPLEMENTACIÓN SEGURA DE EXCHANGE SERVER 2016 SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS".

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

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

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:

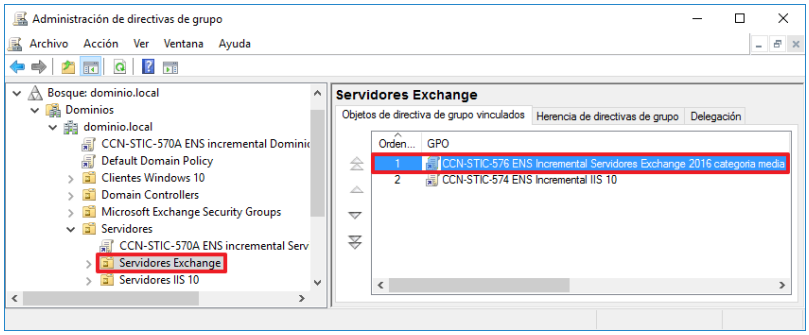
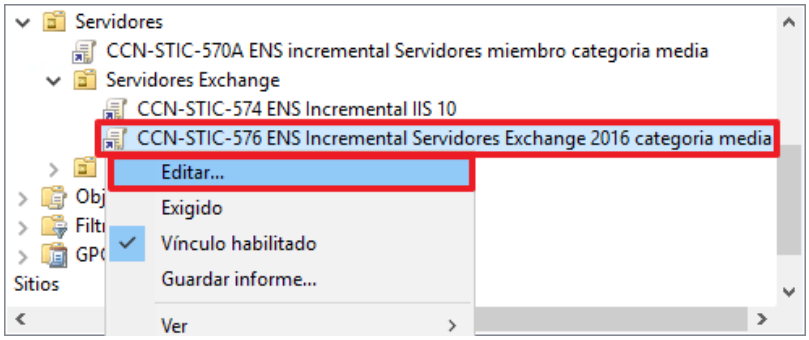
a) Usuarios y equipos de Active Directory (dsa.msc).

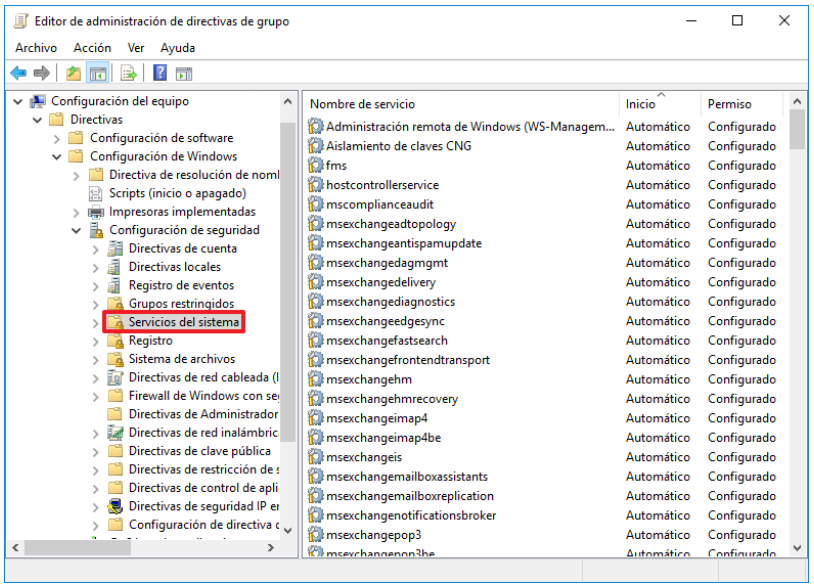
b) Administrador de directivas de grupo (gpmc.msc).

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 un controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.

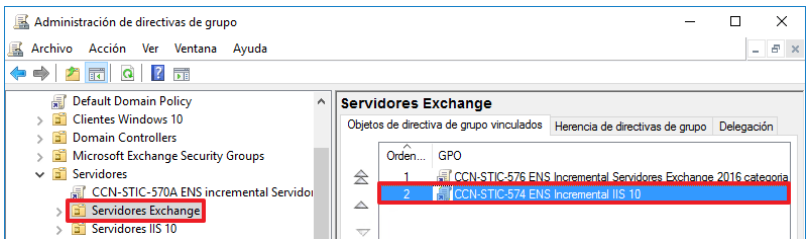
Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que está creada la directiva de Exchange 2016 (CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria media).		Ejecute la herramienta "Administración de directivas de grupo" desde "**Administrador del servidor → Herramientas → Administración de directivas de grupo**". El sistema le solicitará elevación de privilegios para acceder al administrador del servidor. Seleccione la unidad organizativa "Servidores Exchange", situada en **"Bosque → Dominios → [Su_dominio] → Servidores → Servidores Exchange"** y a continuación, en el panel de la derecha, verifique que está creado el objeto de directiva de grupo denominado "CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria media" y se encuentra en el primer orden de directivas de grupo vinculados.  Seleccione con el botón derecho el objeto de directiva de grupo y haga clic en la opción "Editar" del menú para verificar los valores de la directiva "CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria media". 

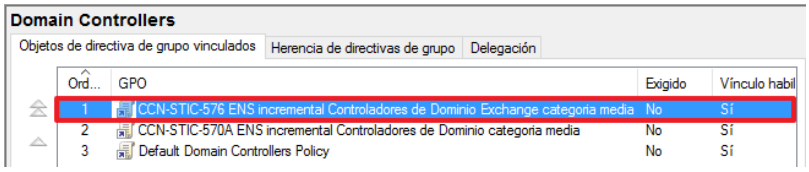
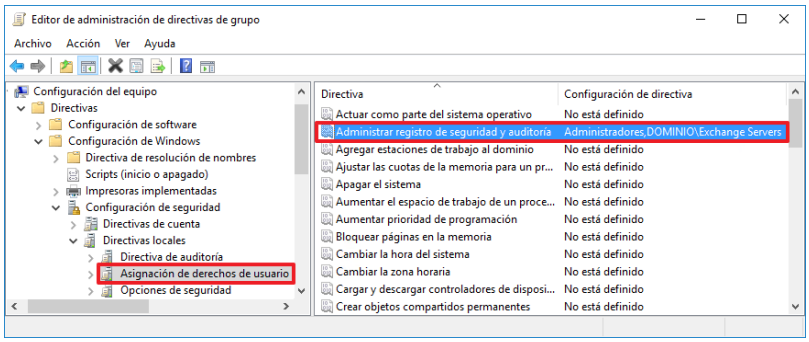
Comprobación	OK/NOK	Cómo hacerlo
3. Verifique los valores de los servicios del sistema de la directiva CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria media.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria media tiene los siguientes valores de servicios de sistema. **"Directiva CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema".**  **Nota:** Puede ordenar los servicios por la columna "Inicio". Dependiendo de los servicios que estén instalados en el controlador de dominio utilizado para la verificación, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales. Cuando finalice, cierre el editor de objetos de directiva de grupo.

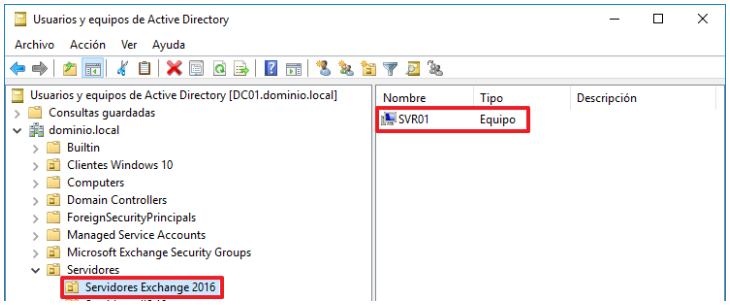
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permisos	OK/NOK
Actualización de correo no deseado de Microsoft Exchange	msexchangeantispamupdate	Automático	Configurado	
Administración de Microsoft Exchange DAG	msexchangedagmgmt	Automático	Configurado	
Administración remota de Windows (WS-Management)	Winrm	Automático	Configurado	
Administrador del estado de Microsoft Exchange	msexchangehm	Automático	Configurado	
Aislamiento de claves CNG	keyiso	Automático	Configurado	
Asistentes de buzón de Microsoft Exchange	msexchangemailboxassistants	Automático	Configurado	
ASP.NET State Service	aspnet_state	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permisos**	**OK/NOK**
Host de servicios de cumplimiento de normas.		msexchangecompliance	Automático	Configurado	
Auditoría de conformidad de Microsoft Exchange		mscomplianceaudit	Automático	Configurado	
Back- end POP3 de Microsoft de Microsoft Exchange		msexchangepop3be	Deshabilitado	Configurado	
Back-end IMAP 4 de Microsoft Exchange		msexchangeimap4be	Deshabilitado	Configurado	
Búsqueda de Microsoft Exchange		msexchangefastsearch	Automático	Configurado	
Diagnósticos de Microsoft Exchange		msexchangediagnostics	Automático	Configurado	
Enrutador de llamadas de mensajería unificada de Microsoft Exchange		msexchangeumcr	Automático	Configurado	
Entrega de transporte de buzones de Microsoft Exchange		msexchangedelivery	Automático	Configurado	
Envío de transporte de buzones de Microsoft Exchange		msexchangesubmission	Automático	Configurado	
Límite de Microsoft Exchange		msexchangethrottling	Automático	Configurado	
Mensajería unificada de Microsoft Exchange		msexchangeum	Automático	Configurado	
Microsoft Exchange EdgeSync		msexchangeedgesync	Automático	Configurado	
Microsoft Exchange IMAP4		msexchangeimap4	Deshabilitado	Configurado	
Microsoft Exchange Information Store		msexchangeis	Automático	Configurado	
Microsoft Exchange Notifications Broker		msexchangenotificationsbroker	Automático	Configurado	
Microsoft Exchange POP3		msexchangepop3	Deshabilitado	Configurado	
Microsoft Exchange Search Host Controller		hostcontrollerservice	Automático	Configurado	
Microsoft Exchange Server Extension for Windows Server Backup		wsbexchange	Manual	Configurado	
Microsoft Exchange Service Host		msexchangeservicehost	Automático	Configurado	
Notificaciones del servicio de token de Windows		c2wts	Manual	Configurado	
Recuperación del administrador del estado de Microsoft Exchange		msexchangehmrecovery	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	**Servicio (nombre corto)**		**Inicio**	**Permisos**	**OK/NOK**
Registro de búsquedas de Transport de Microsoft Exchange	msexchangetransportlogsearch		Automático	Configurado	
Registro remoto	remoteregistry		Automático	Configurado	
Replicación de buzón de Microsoft Exchange	msexchangemailboxreplication		Automático	Configurado	
Replicación de Microsoft Exchange	msexchangerepl		Automático	Configurado	
Servicio de acceso de cliente RPC de Microsoft Exchange	msexchangerpc		Automático	Configurado	
Servicio de administración de filtrado de Microsoft	fms		Automático	Configurado	
Servicio de equilibrio de carga RPC/HTTP	rpchttplbs		Manual	Configurado	
Servicio de uso compartido de puertos Net.Tcp	nettcpportsharing		Automático	Configurado	
Servicio WAS (Windows Process Activation Service)	was		Automático	Configurado	
Servidor	lanmanserver		Automático	Configurado	
Sistema de eventos COM+	eventsystem		Manual	Configurado	
Topología de Active Directory de Microsoft Exchange	msexchangeadtopology		Automático	Configurado	
Tracing Service for Search in Exchange	searchexchangetracing		Automático	Configurado	
Transport de Microsoft Exchange	msexchangetransport		Automático	Configurado	
Transporte Frontend de Microsoft Exchange	msexchangefrontendtransport		Automático	Configurado	

4. Verifique que está creada la directiva de Internet Information Services 10 (CCN-STIC-574 ENS Incremental IIS 10).		Sin salir de la consola "Administración de directivas de grupo", seleccione la unidad organizativa "Servidores Exchange", situada en **"Bosque → Dominios → [Su_dominio] → Servidores → Servidores Exchange"** y a continuación, verifique que está creado el objeto de directiva de grupo denominado "CCN-STIC-574 ENS Incremental IIS 10".  **Nota:** La configuración de seguridad de esta GPO deberá de haberse comprobado en la guía codificada como "CCN-STIC-574".

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>5. Verifique que está creada la directiva CCN-STIC-576 ENS Incremental Controladores de Dominio Exchange categoria media.</td><td></td><td>Sin salir de la consola “Administración de directivas de grupo”, seleccione la unidad organizativa “Servidores Exchange”, situada en “Bosque → Dominios → [Su_dominio] → Domain Controllers” y a continuación, verifique que está creado el objeto de directiva de grupo denominado “CCN-STIC-576 ENS Incremental Controladores de Dominio Exchange categoria media” y se encuentra en el primer orden de vínculos.
 
</td></tr>
<tr><td>6. Verifique los valores de seguridad de la directiva CCN-STIC-576 ENS Incremental Controladores de Dominio Exchange categoria media.</td><td></td><td>Utilizando el editor de objetos de directiva de grupo, verifique que la directiva “CCN-STIC-576 Incremental Controlador de Dominio Exchange categoria media” tiene el siguiente valor de seguridad.
“CCN-STIC-576 ENS Incremental Controladores de Dominio Exchange → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Administrar registro de seguridad y auditoría</td><td>Administradores Exchange Servers</td><td></td></tr>
</table></td></tr>
<tr><td>7. Verifique que los servidores a asegurar están dentro de la unidad organizativa “Servidores Exchange”.</td><td></td><td>Ejecute la herramienta “Usuarios y equipos de Active Directory” desde “Administrador del servidor → Herramientas → Usuarios y equipos de Active Directory”. El sistema le solicitará elevación de privilegios para acceder al administrador del servidor.
A continuación, seleccione la unidad organizativa “Servidores Exchange” y verifique que se encuentra el servidor donde se ha instalado Exchange Server 2016.
 
</td></tr>
</table>

2. COMPROBACIONES EN SERVIDOR MIEMBRO

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:

a) Administrador de Windows (explorer.exe).

b) Símbolo del sistema (cmd.exe).

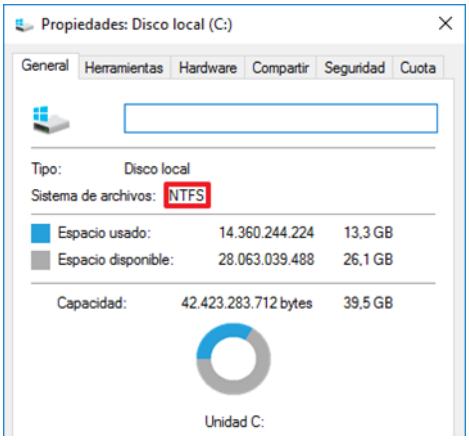
c) Servicios (services.msc).

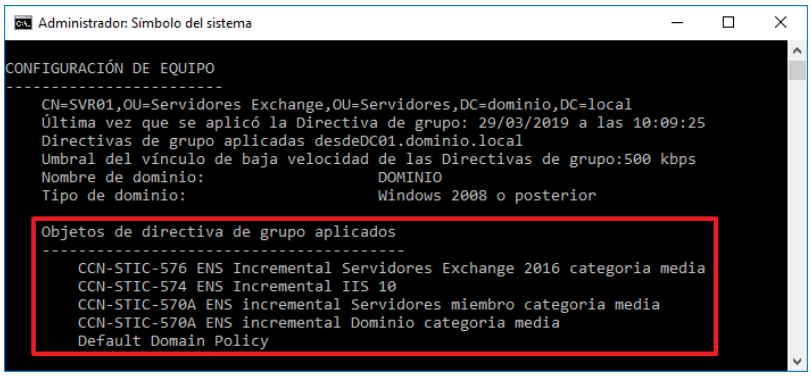
d) Editor de objetos de directiva de grupo (gpedit.msc).

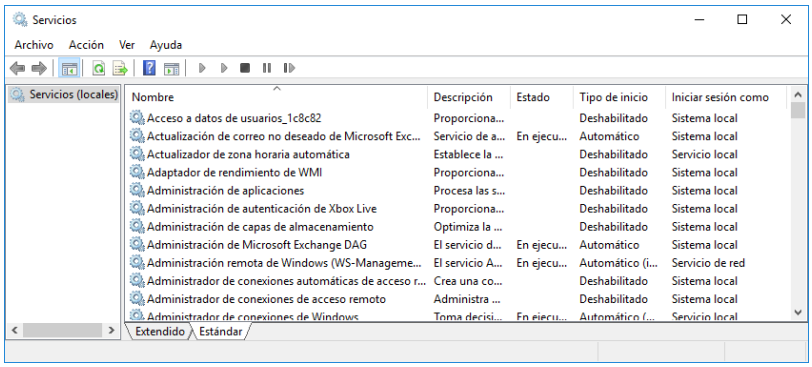
e) Administrador de Internet Information Services (iis.msc).

f) Consola Web de administración de Exchange 2016.

g) Shell de administración de Exchange 2016.

Comprobación	OK/NOK	Cómo hacerlo
8. Inicie sesión en los servidores Exchange 2016.		A continuación, para completar el resto de la lista de comprobación deberá iniciar sesión en el servidor donde se aloja Exchange Server 2016 con una cuenta que tenga permisos de administrador local del servidor, administrador del dominio o administrador de la organización de Exchange.
9. Verifique que todos los volúmenes están formateados con NTFS.		Utilizando el explorador de Windows (botón derecho sobre **Inicio → Explorador de archivos, botón derecho sobre la unidad C:\ → Propiedades**), verifique en las propiedades de cada partición el uso del sistema de archivos NTFS o cualquier sistema de archivos que permita ACL's. 

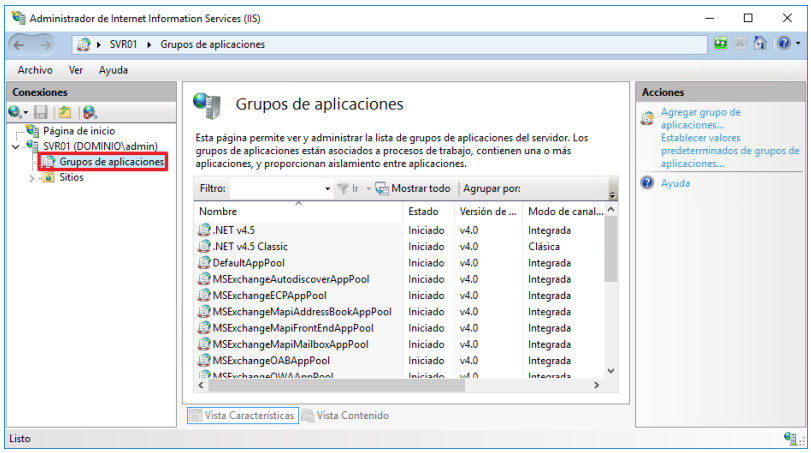
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>10. Verifique que le están aplicando las GPO de forma correcta.</td><td></td><td>Abra una consola de comandos como administrador con botón derecho en “Inicio → Símbolo del sistema (administrador)” y ejecute el comando “gpresult –r”. Compruebe que las GPO están aplicando al equipo en el orden correcto.
 

<table>
<tr><th>Objeto de directiva de grupo</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria media</td><td></td></tr>
<tr><td>CCN-STIC-574 ENS Incremental IIS 10</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS incremental Servidores miembro categoria media</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS Incremental Dominio categoria media</td><td></td></tr>
<tr><td>Default Domain Policy</td><td></td></tr>
</table></td></tr>
<tr><td>11. Verifique que los servicios del sistema están configurados de forma correcta.</td><td></td><td>Ejecute la herramienta “Servicios” desde “Administrador del servidor → Herramientas → Servicios”. El sistema le solicitará elevación de privilegios para acceder al administrador del servidor.
 

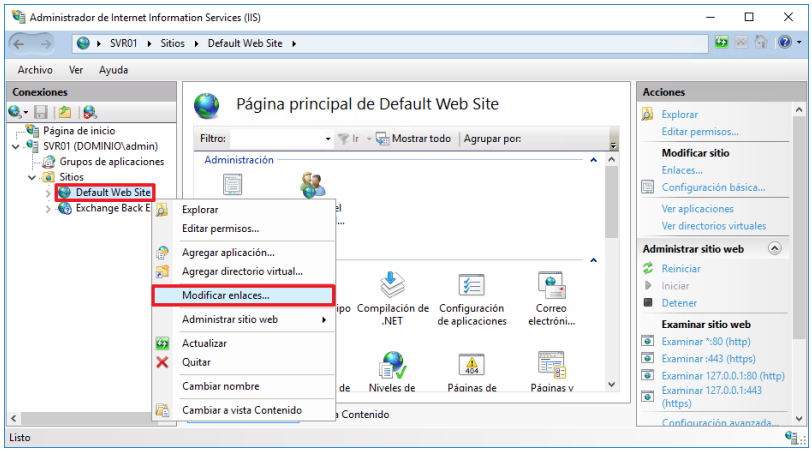
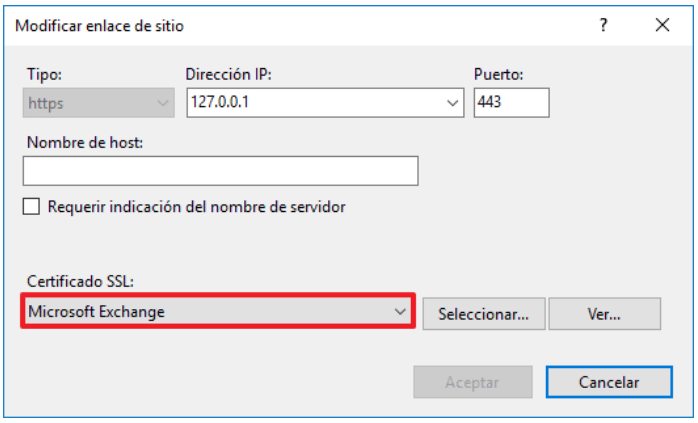
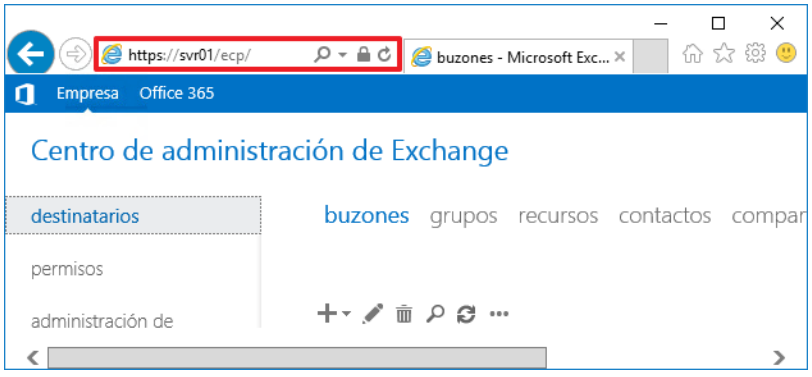
Nota: Dependiendo del equipo, es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales. Puede ordenar los servicios por “Tipo de inicio”. Sólo se verifican los servicios que configura esta guía.</td></tr>
</table>

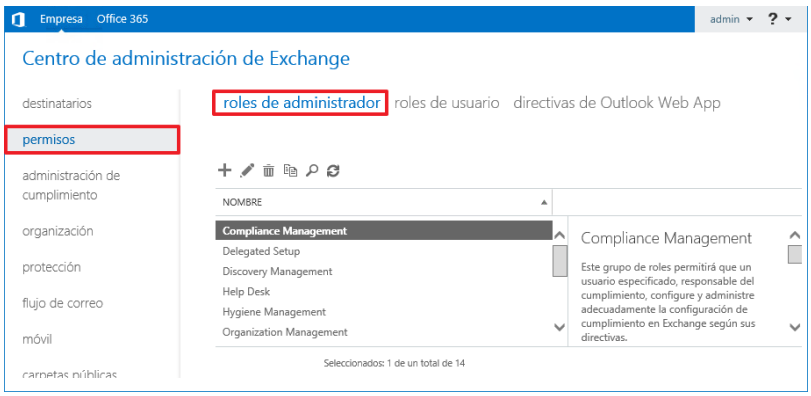
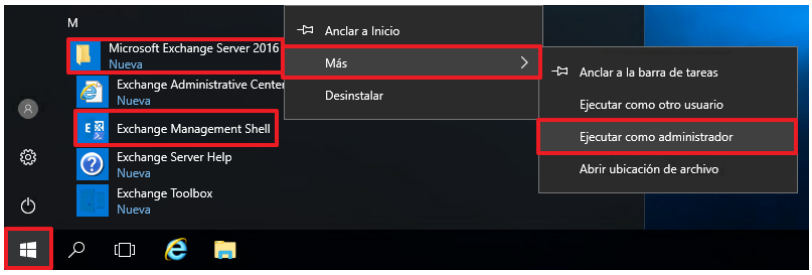
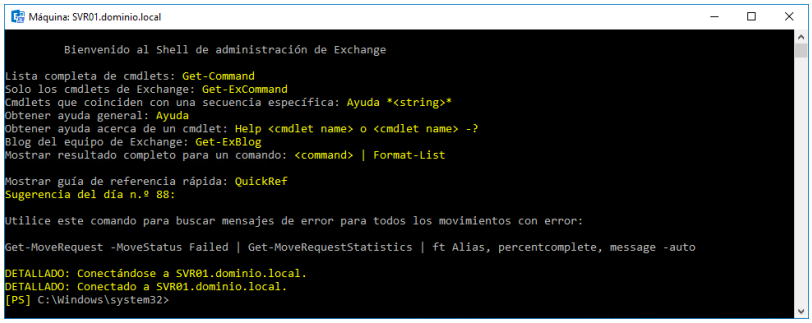
Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permisos**	**OK/NOK**	
Actualización de correo no deseado de Microsoft Exchange	msexchangeantispamupdate	Automático	Configurado		
Administración de Microsoft Exchange DAG	msexchangedagmgmt	Automático	Configurado		
Administración remota de Windows (WS-Management)	winrm	Automático	Configurado		
Administrador del estado de Microsoft Exchange	msexchangehm	Automático	Configurado		
Aislamiento de claves CNG	keyiso	Automático	Configurado		
Asistentes de buzón de Microsoft Exchange	msexchangemailboxassistants	Automático	Configurado		
ASP.NET State Service	aspnet_state	Manual	Configurado		
Auditoría de conformidad de Microsoft Exchange	mscomplianceaudit	Automático	Configurado		
Servicio de cumplimiento de normas de Microsoft Exchange.	msexchangecompliance	Automático	Configurado		
Back- end POP3 de Microsoft de Microsoft Exchange	msexchangepop3be	Deshabilitado	Configurado		
Back-end IMAP 4 de Microsoft Exchange	msexchangeimap4be	Deshabilitado	Configurado		
Búsqueda de Microsoft Exchange	msexchangefastsearch	Automático	Configurado		
Diagnósticos de Microsoft Exchange	msexchangediagnostics	Automático	Configurado		
Enrutador de llamadas de mensajería unificada de Microsoft Exchange	msexchangeumcr	Automático	Configurado		
Entrega de transporte de buzones de Microsoft Exchange	msexchangedelivery	Automático	Configurado		
Envío de transporte de buzones de Microsoft Exchange	msexchangesubmission	Automático	Configurado		
Límite de Microsoft Exchange	msexchangethrottling	Automático	Configurado		
Mensajería unificada de Microsoft Exchange	msexchangeum	Automático	Configurado		
Microsoft Exchange EdgeSync	msexchangeedgesync	Automático	Configurado		
Microsoft Exchange IMAP4	msexchangeimap4	Deshabilitado	Configurado		
Microsoft Exchange Information Store	msexchangeis	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permisos**	**OK/NOK**	
Microsoft Exchange Notifications Broker	msexchangenotificationsbroker	Automático	Configurado		
Microsoft Exchange POP3	msexchangepop3	Deshabilitado	Configurado		
Microsoft Exchange Search Host Controller	hostcontrollerservice	Automático	Configurado		
Microsoft Exchange Server Extension for Windows Server Backup	wsbexchange	Manual	Configurado		
Microsoft Exchange Service Host	msexchangeservicehost	Automático	Configurado		
Notificaciones del servicio de token de Windows	c2wts	Manual	Configurado		
Recuperación del administrador del estado de Microsoft Exchange	msexchangehmrecovery	Automático	Configurado		
Registro de búsquedas de Transport de Microsoft Exchange	msexchangetransportlogsearch	Automático	Configurado		
Registro remoto	remoteregistry	Automático	Configurado		
Replicación de buzón de Microsoft Exchange	msexchangemailboxreplication	Automático	Configurado		
Replicación de Microsoft Exchange	msexchangerepl	Automático	Configurado		
Servicio de acceso de cliente RPC de Microsoft Exchange	msexchangerpc	Automático	Configurado		
Servicio de administración de filtrado de Microsoft	fms	Automático	Configurado		
Servicio de equilibrio de carga RPC/HTTP	rpchttplbs	Manual	Configurado		
Servicio de uso compartido de puertos Net.Tcp	nettcpportsharing	Automático	Configurado		
Servicio WAS (Windows Process Activation Service)	was	Automático	Configurado		
Servidor	lanmanserver	Automático	Configurado		
Sistema de eventos COM+	eventsystem	Manual	Configurado		
Topología de Active Directory de Microsoft Exchange	msexchangeadtopology	Automático	Configurado		
Tracing Service for Search in Exchange	searchexchangetracing	Automático	Configurado		
Transport de Microsoft Exchange	msexchangetransport	Automático	Configurado		
Transporte Frontend de Microsoft Exchange	msexchangefrontendtransport	Automático	Configurado		

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>12. En el servidor Exchange, verifique que se han creado los grupos de aplicaciones correspondientes.</td><td></td><td>Ejecute la herramienta “Administrador de Internet Information Services (IIS)” desde “Administrador del servidor → Herramientas → Administrador de Internet Information Services (IIS)”. El sistema le solicitará elevación de privilegios para acceder al administrador del servidor.
Seleccione el nodo “Nombre_Servidor → Grupo de aplicaciones” y verifique que existen los siguientes grupos de aplicaciones de Exchange.
 

<table>
<tr><th>Grupos de aplicaciones</th><th>OK/NOK</th></tr>
<tr><td>.Net v4.5</td><td></td></tr>
<tr><td>.Net v4.5 Classic</td><td></td></tr>
<tr><td>DefaultAppPool</td><td></td></tr>
<tr><td>MSExchangeAutodiscoverAppPool</td><td></td></tr>
<tr><td>MSExchangeECPAppPool</td><td></td></tr>
<tr><td>MSExchangeMAPIAddressBookAppPool</td><td></td></tr>
<tr><td>MSExchangeMAPIFrontEndAppPool</td><td></td></tr>
<tr><td>MSExchangeMAPIMailboxAppPool</td><td></td></tr>
<tr><td>MSExchangeOABAppPool</td><td></td></tr>
<tr><td>MSExchangeOWAAppPool</td><td></td></tr>
<tr><td>MSExchangeOWACalendarAppPool</td><td></td></tr>
<tr><td>MSExchangePowerShellAppPool</td><td></td></tr>
<tr><td>MSExchangePowerShellFrontEndAppPool</td><td></td></tr>
<tr><td>MSExchangePushNotificationsAppPool</td><td></td></tr>
<tr><td>MSExchangeRestAppPool</td><td></td></tr>
<tr><td>MSExchangeRestFrontEndAppPool</td><td></td></tr>
<tr><td>MSExchangeRPCProxyAppPool</td><td></td></tr>
<tr><td>MSExchangeRPCProxyFrontEndAppPool</td><td></td></tr>
<tr><td>MSExchangeServicesAppPool</td><td></td></tr>
<tr><td>MSExchangeSyncAppPool</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
13. En el servidor Exchange, verifique que se ha establecido el certificado correspondientes.		En la herramienta "Administrador de Internet Information Services (IIS)" seleccione con botón derecho el nodo **"Nombre_Servidor → Sitios → Default Web Site"** y pulse sobre "Modificar enlaces…".  Confirme que está seleccionado el certificado SSL correcto en el enlace de tipo https con puerto 443. 
14. Verifique el acceso la consola Web de Exchange Server 2016 se realiza de forma correcta.		Inicie sesión en la consola de administración de Exchange desde el navegador.  **Nota:** En este ejemplo se usa https://SVR01/ecp.

Comprobación	OK/NOK	Cómo hacerlo
15. Confirme que se ha creado un grupo de auditoría.		Pulse en **"Permisos → roles de administrador"** y confirme que se han aplicado los permisos adecuados a su organización. 
16. En el servidor Exchange, verifique el acceso correcto al Shell de Exchange Server 2016.		Inicie sesión en el Shell de administración de Exchange desde el menú **"Inicio → Todas las aplicaciones → Microsoft Exchange Server 2016"** y pulse con botón derecho en "Exchange Management Shell". El sistema le solicitará elevación de privilegios.  Tras introducir las credenciales, compruebe que se ejecute "Exchange Management Shell" correctamente como aparece en la siguiente imagen. 

ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

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

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas, a realizar una implementación de seguridad en escenarios donde se emplee el producto Microsoft Exchange Server 2016 sobre Windows Server 2016, con una categorización de seguridad alta según los criterios del Esquema Nacional de Seguridad.

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

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

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

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

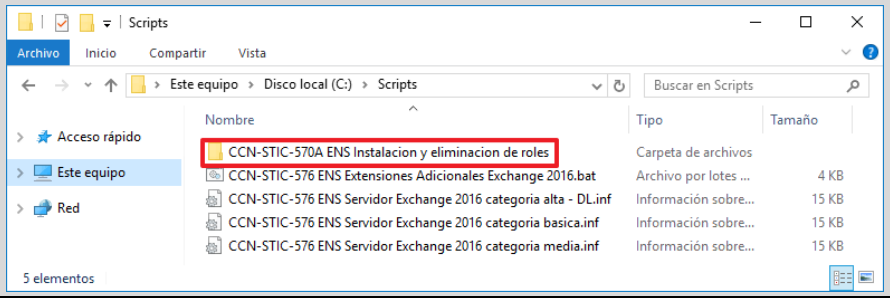
Microsoft Exchange Server 2016 requiere de otros servicios adicionales para su instalación y correcto funcionamiento, por lo que es necesario realizar una preparación previa del entorno antes de instalar Microsoft Exchange Server 2016

En caso de necesitar información sobre los requisitos previos de instalación de Microsoft Exchange Server 2016, visite el siguiente enlace: https://docs.microsoft.com/es-es/Exchange/plan-and-deploy/prerequisites?view=exchserver -2016

a) Un servidor controlador de dominio Windows Server 2016 que haya sido preparado siguiendo la guía de seguridad CCN-STIC-570A Anexo A con una categorización de seguridad alta - DL.

b) Un servidor miembro del dominio con el servicio Web Internet Information Services instalado y preparado siguiendo las guías CCN-STIC-570A Anexo A y CCN-STIC-574 Anexo A con una categorización de seguridad alta - DL.

Nota: Si instala Exchange 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.

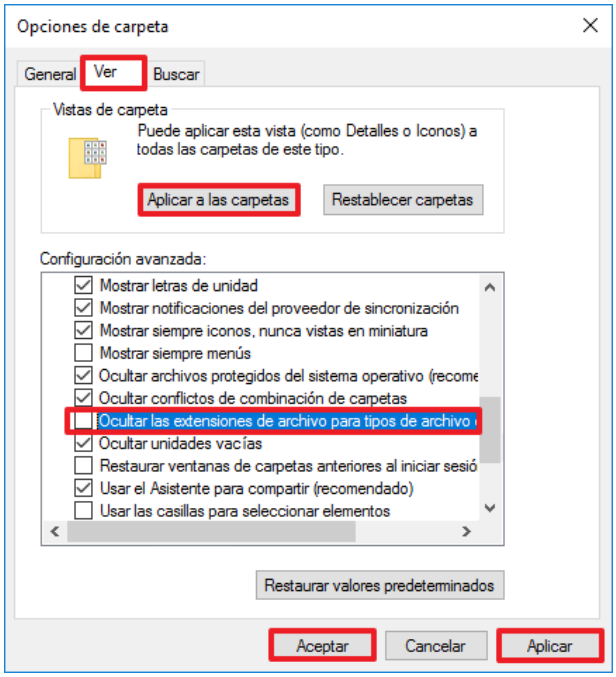


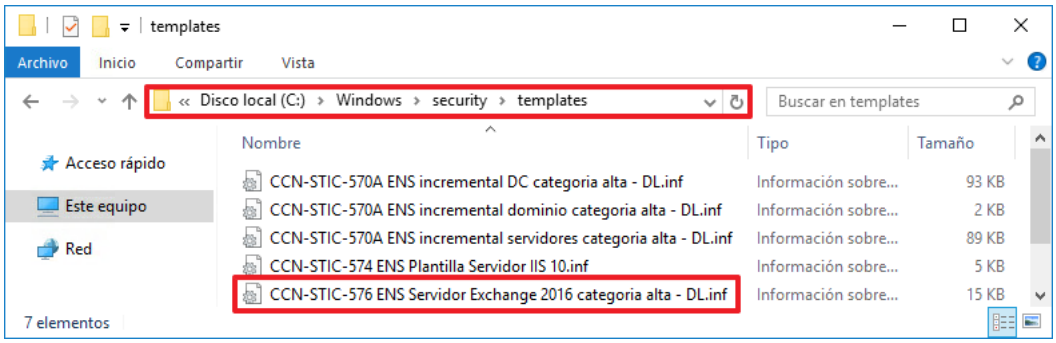
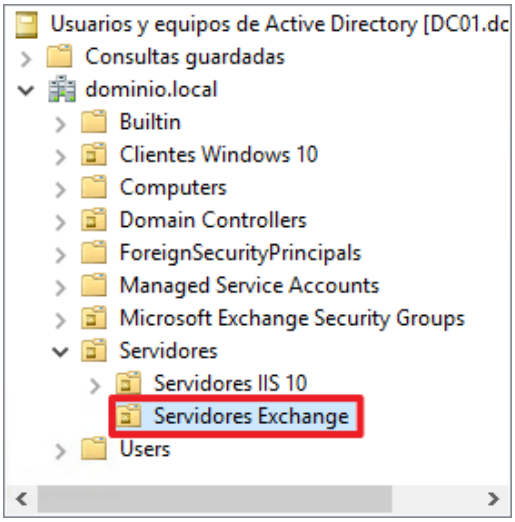
1. PREPARACIÓN DEL DOMINIO

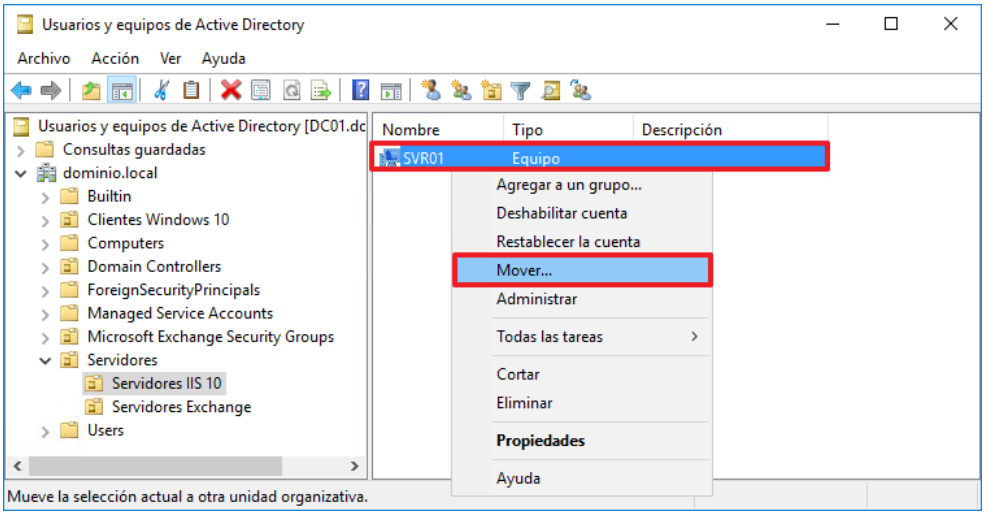
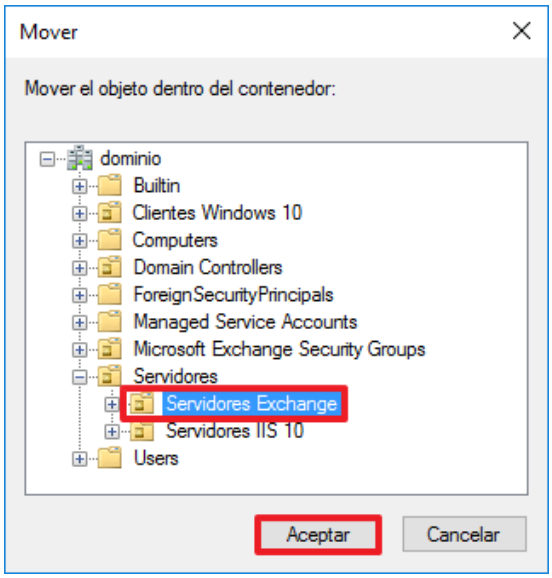
Los pasos que se describen a continuación se realizarán en un controlador del dominio al que va a pertenecer el servidor miembro que contenga Microsoft Exchange Server 2016. Estos pasos sólo se realizarán cuando se incluya el primer servidor de Microsoft Exchange Server 2016 que actúe como miembro del dominio. Durante este procedimiento se crea la unidad organizativa que contiene los servidores de correo y se realizan las configuraciones de políticas de grupo correspondientes.

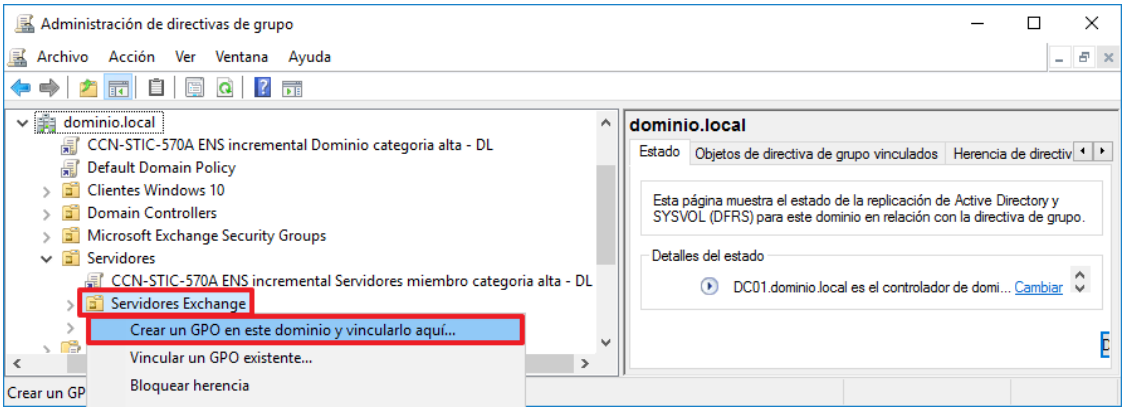
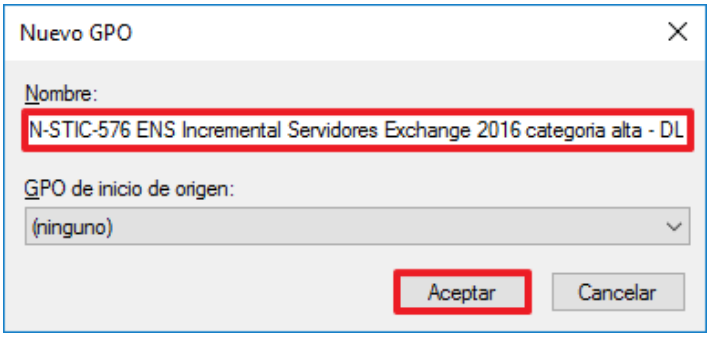
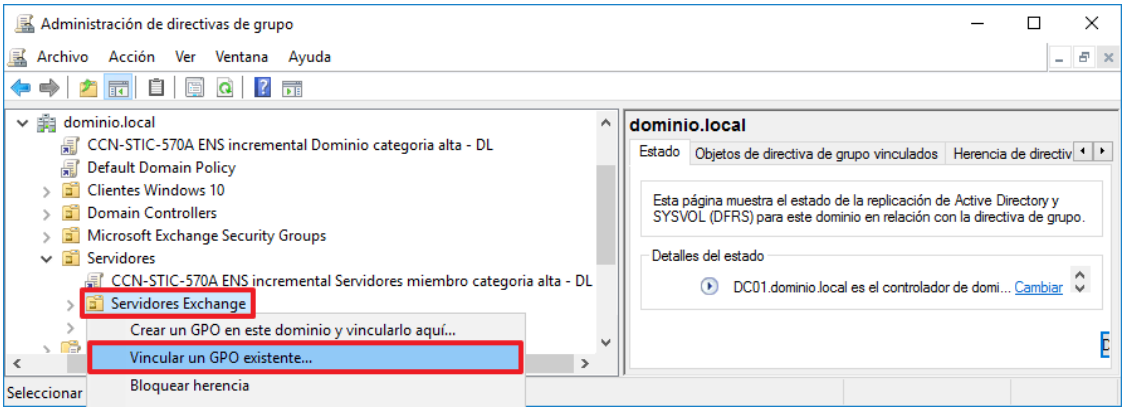
Nota: Esta guía asume que los servidores Controladores del Dominio al que pertenece el equipo servidor de Exchange que está asegurando, se les ha aplicado la configuración descrita en la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016". Si no es así, aplique la guía correspondiente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

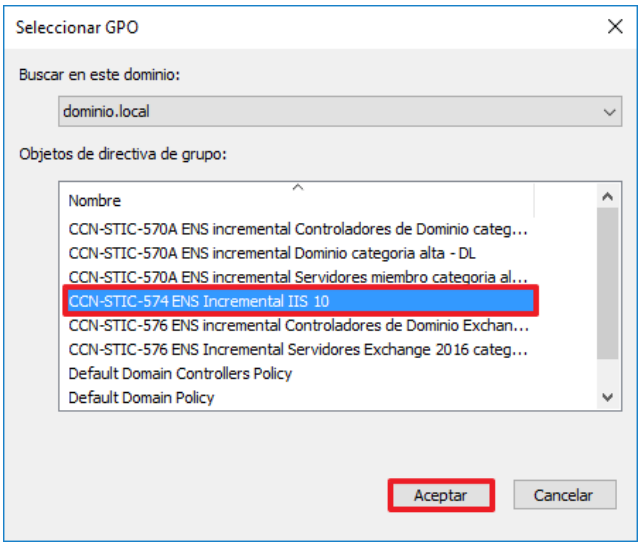
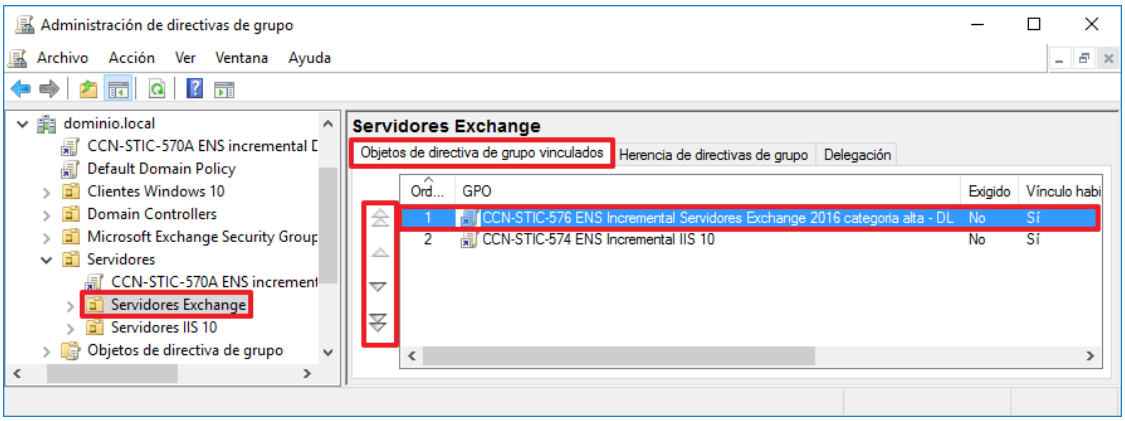
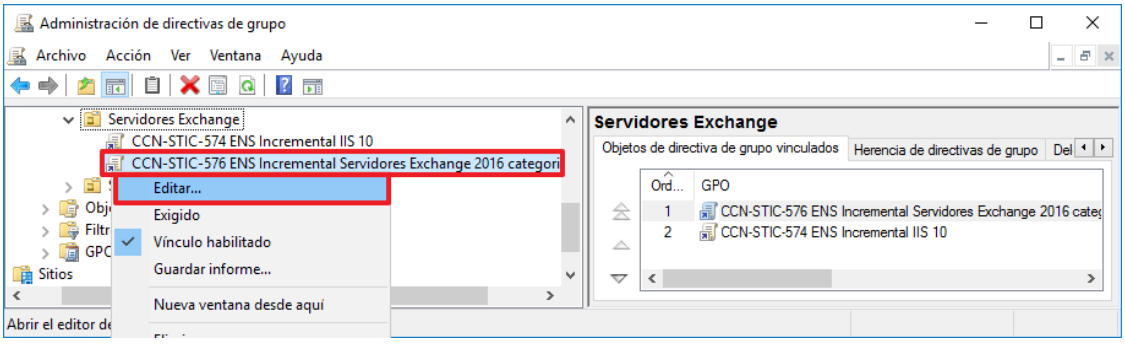
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.

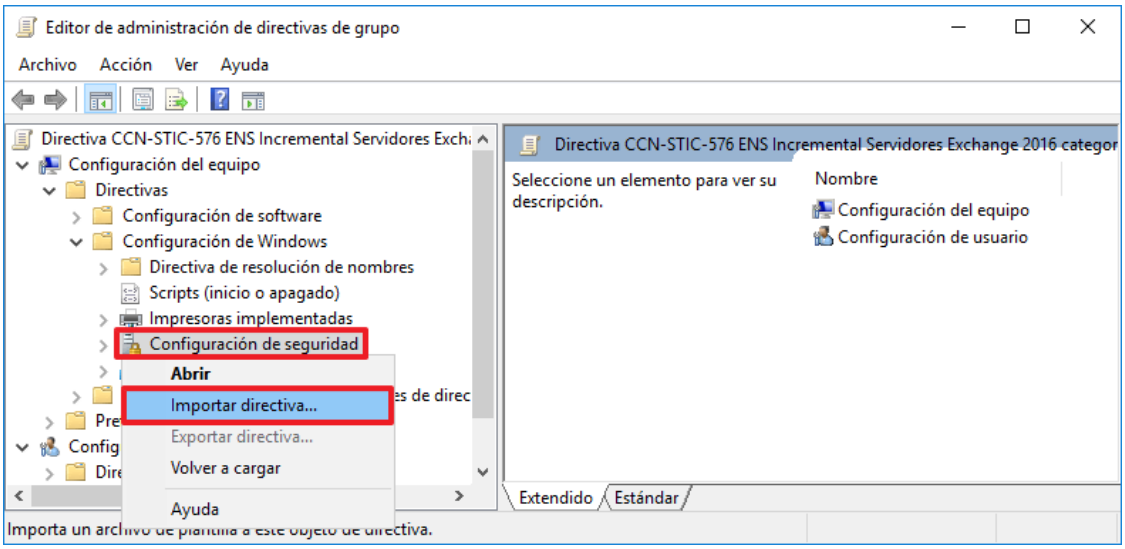
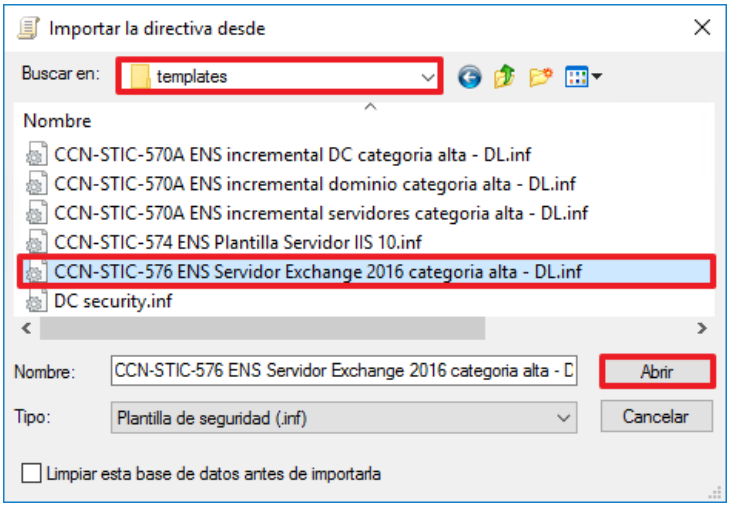
Paso	Descripción
2.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.
4.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos.
5.	Para configurar el “Explorador de Windows” de modo que muestre las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones" de la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

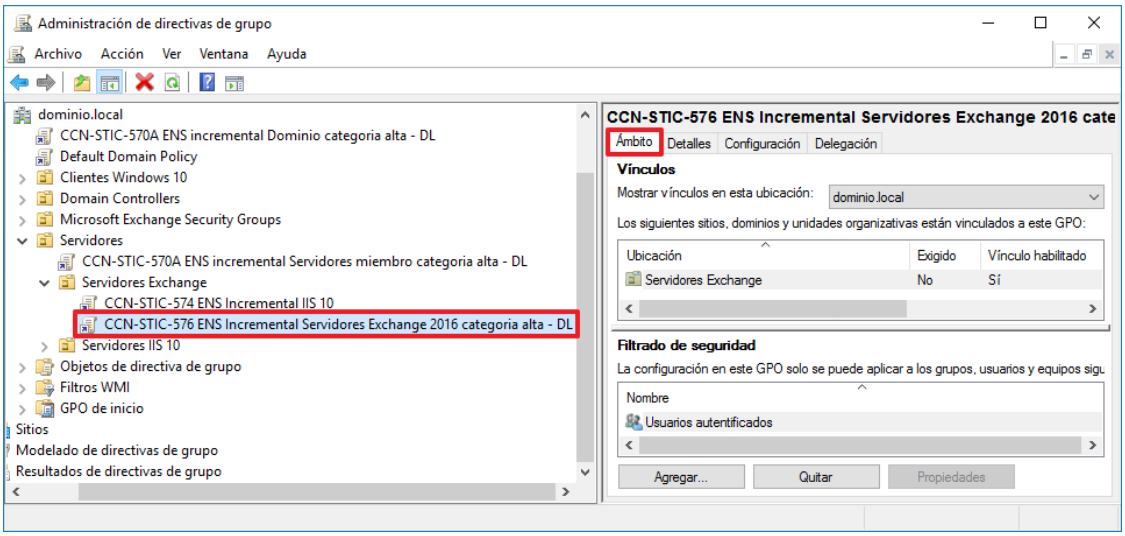
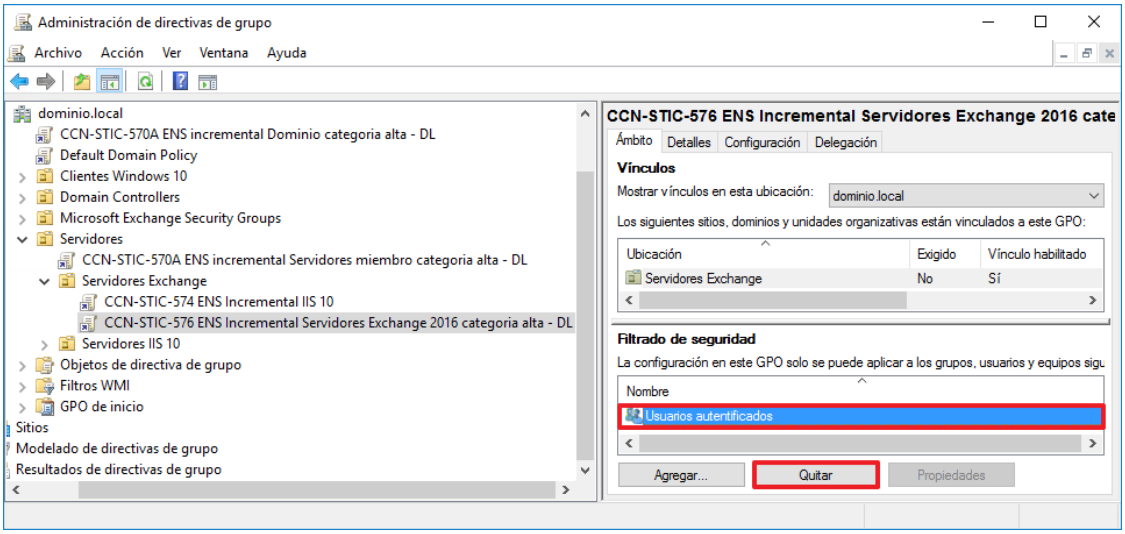
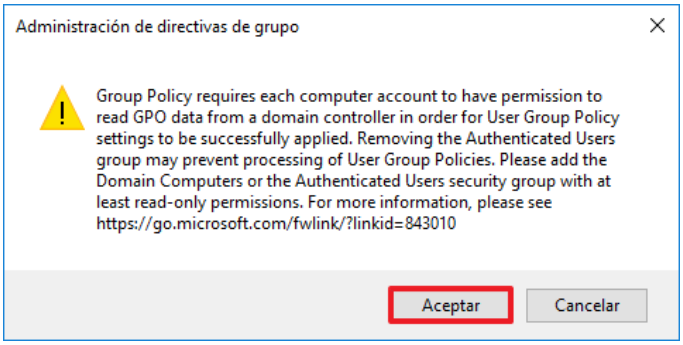
Paso	Descripción
6.	Copie los ficheros "CCN-STIC-576 ENS Servidor Exchange 2016 categoria alta - DL.inf" al directorio "C:\Windows\Security\Templates" del Controlador de Dominio.  **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón "Continuar" e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. En este ejemplo y durante todo el paso a paso se hará uso de la cuenta "DOMINIO\Admin".
7.	Ejecute la consola administrativa Usuarios y Equipos de Directorio Activo desde el Administrador del servidor **"Herramientas → Usuarios y Equipos de Active Directory"**. **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el menú de inicio. Si lo inicia por primera vez, el control de cuentas de usuario le solicitará permiso para iniciar el administrador del servidor.
8.	En la consola, cree una nueva unidad organizativa denominada "Servidores Exchange" dependiendo de la unidad organizativa "Servidores", tal y como se muestra en la imagen.  **Nota:** En este ejemplo se crea la nueva unidad organizativa bajo "Servidores". Modifique este paso de acuerdo con las necesidades del entorno de su organización.

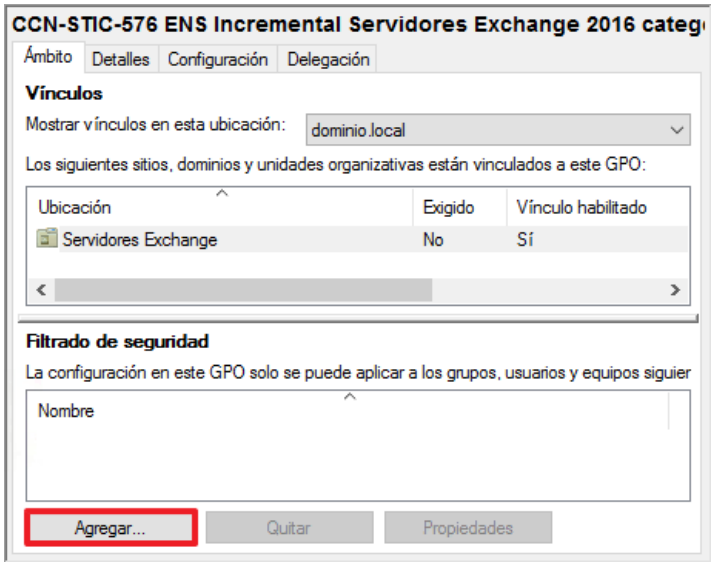
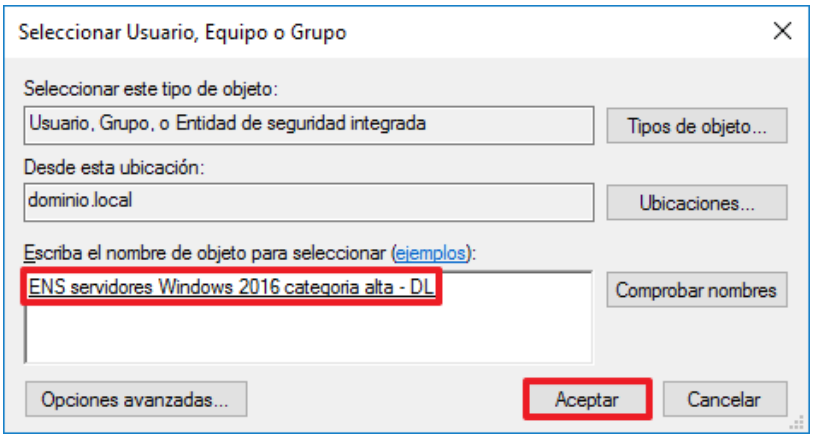
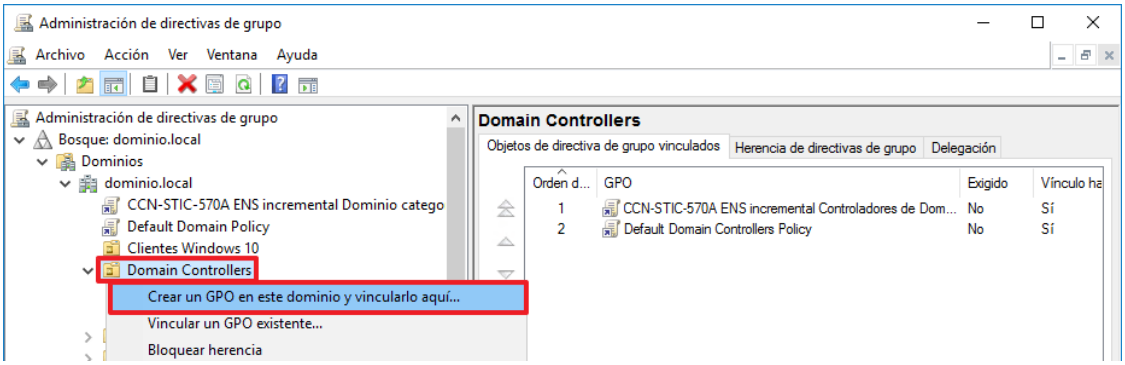
Paso	Descripción
9.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores que contengan Exchange Server 2016 a la unidad organizativa "Servidores Exchange". Para ello, deberá hacer clic botón derecho sobre "Mover" en el servidor que desee ubicar en la nueva unidad organizativa.  **Nota:** Si ha seguido los pasos de la guía "CCN-STIC-574 Implementación del ENS en IIS 10 sobre Windows Server 2016" el servidor se encontrará bajo la unidad organizativa "Servidores IIS 10".
10.	A continuación, seleccione la unidad organizativa "Servidores Exchange". 
11.	Cierre la herramienta de "Usuarios y equipos de Directorio Activo"
12.	Una vez realizada la preparación del Directorio Activo que dará servicio a Exchange Server 2016, deberá realizar el resto de preparación y configuración de políticas de seguridad. Para ello, inicie la consola de administración de directivas de grupo desde el Administrador del servidor en el menú **"Herramientas → Administración de directivas de grupo"**.

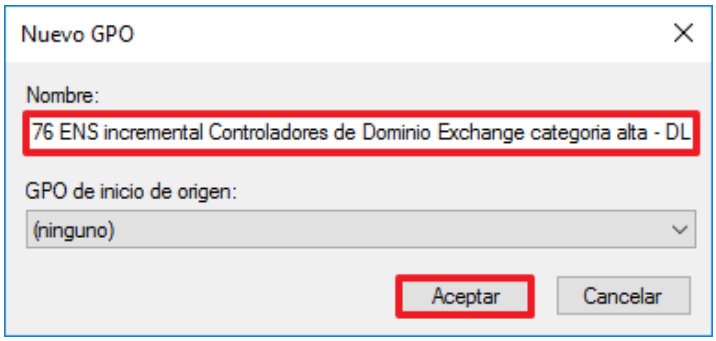
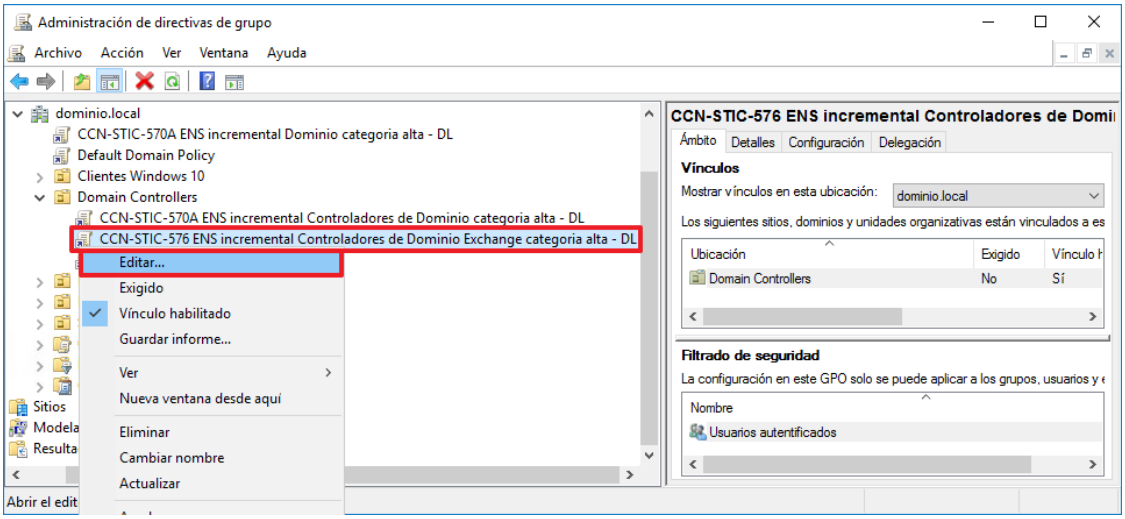
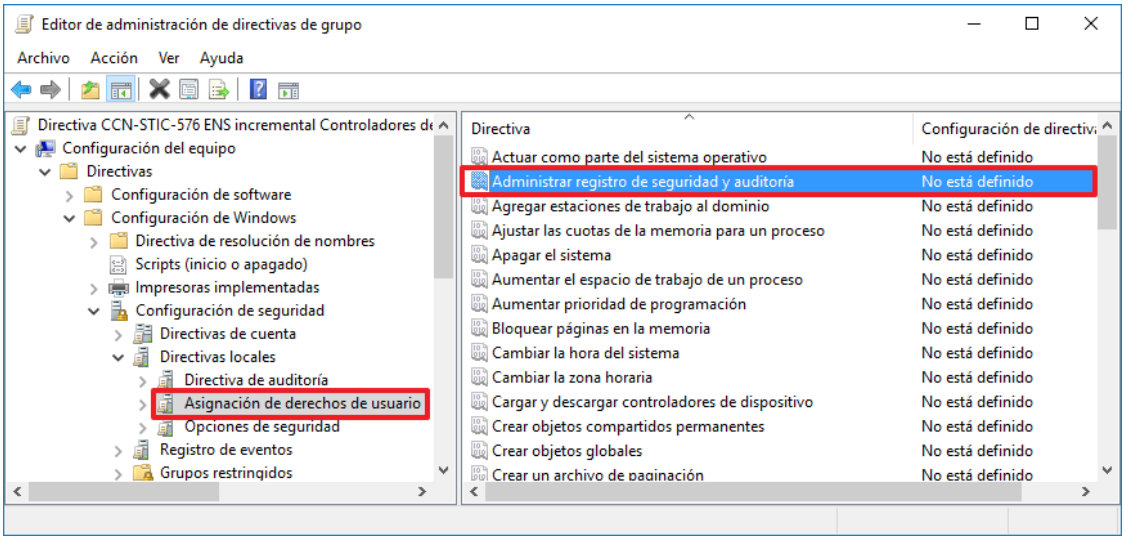
Paso	Descripción
13.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa recién creada "Servidores Exchange", haciendo clic con el botón derecho en el menú "Crear un GPO en este dominio y vincularlo aquí…". 
14.	Escriba el nombre de la GPO "CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria alta - DL" y haga clic en el botón "Aceptar". 
15.	A continuación, se va a vincular la GPO "CCN-STIC-574 ENS Incremental IIS 10" de la guía "CCN-STIC-574 Implementación del ENS en IIS 10 sobre Windows Server 2016", en la unidad organizativa "Servidores Exchange" creada en pasos anteriores.
16.	Pulse botón derecho sobre la unidad organizativa "Servidores Exchange" y haga clic sobre "Vincular un GPO existente…". 

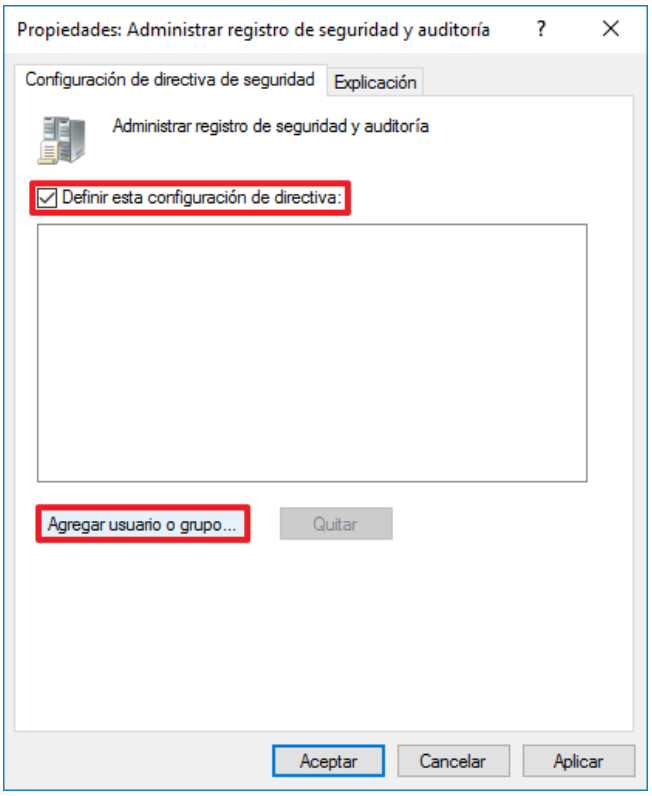
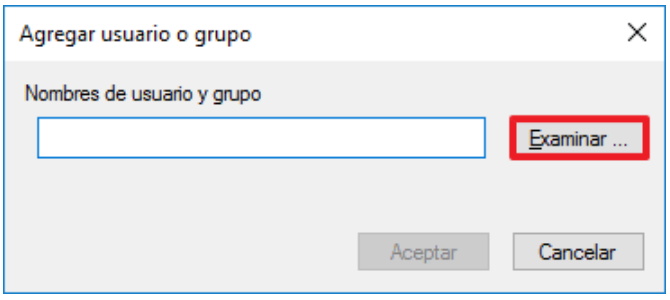
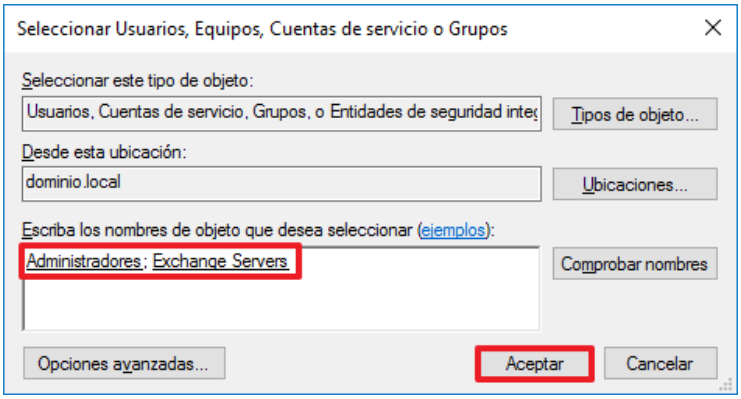
Paso	Descripción
17.	A continuación, seleccione el objeto de directiva de grupo: "CCN-STIC-574 ENS Incremental IIS 10" y pulse sobre "Aceptar". 
18.	Para que la aplicación de las directivas se realice en el orden correcto, asegúrese de que la directiva "CCN-STIC-576 ENS Incremental Servidor Exchange 2016 categoria alta - DL" aparezca en primer lugar. Para ello seleccione, dentro de la unidad organizativa, la directiva "CCN-STIC-576 ENS Incremental Servidor Exchange 2016 categoria alta - DL" y a continuación, haga clic sobre la flecha doble hacia arriba para que se sitúe en primer lugar del orden vínculos, tal y como se muestra en la imagen. 
19.	A continuación, edite la GPO: "CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria alta - DL" creada anteriormente haciendo clic con el botón derecho en ella y seleccionando el menú "Editar". 

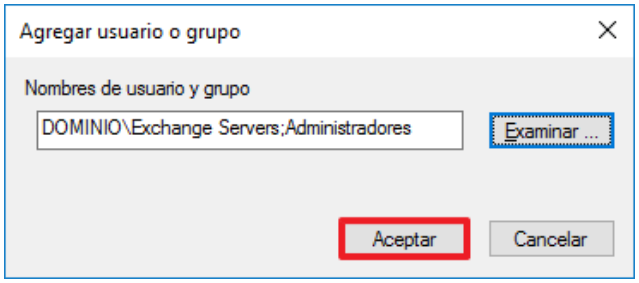
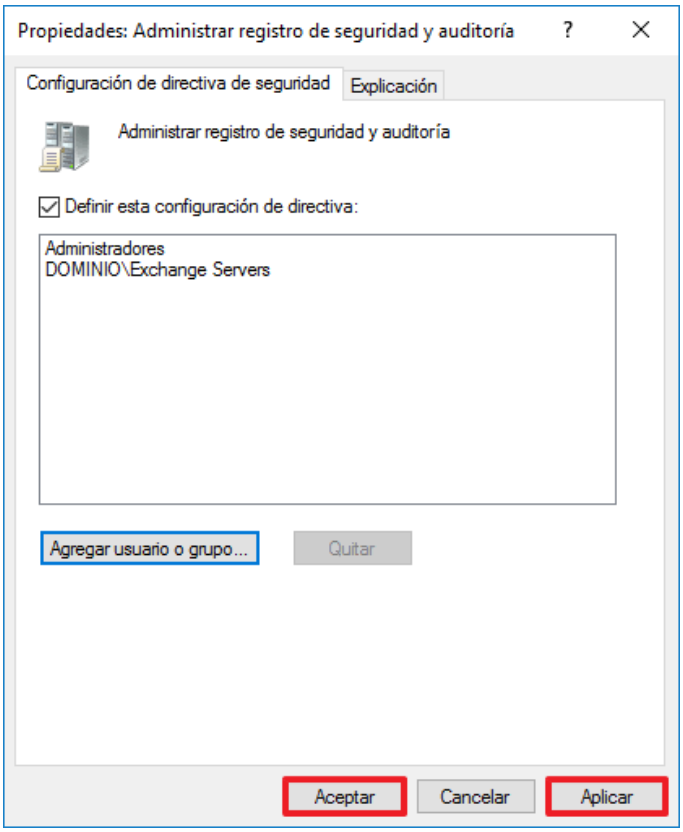
Paso	Descripción
20.	Expanda el nodo **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad"**.
21.	A continuación, haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 
22.	Importe la plantilla de seguridad "CCN-STIC-576 ENS Servidor Exchange 2016 categoria alta - DL.inf" que previamente debe haberse copiado en la ruta "C:\Windows\Security\Templates" y haga clic en botón "Abrir". 
23.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.

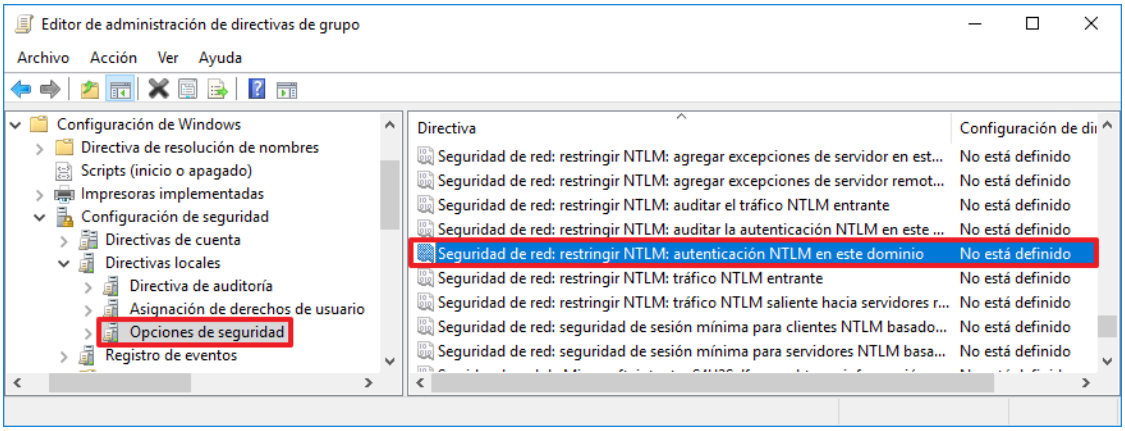
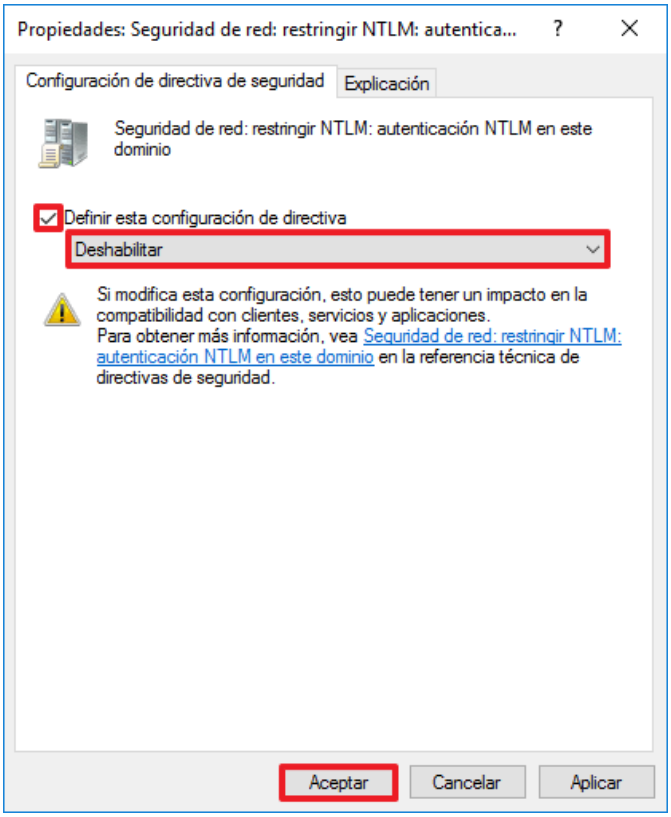
Paso	Descripción
24.	Seleccione la nueva política de grupo configurada y vaya a la pestaña "Ámbito" que se encuentra en el panel derecho. 
25.	En la opción de filtrado de seguridad, seleccione "Usuarios autentificados" y pulse la opción "Quitar". 
26.	Pulse el botón "Aceptar" cuando le pregunte si desea quitar este privilegio de delegación.
27.	Pulse "Aceptar" sobre la advertencia que se mostrará en una ventana emergente. 

Paso	Descripción
28.	Una vez quitado, pulse el botón "Agregar…". 
29.	Introduzca como nombre "ENS servidores Windows 2016 categoria alta - DL". Este grupo corresponde con el generado en la aplicación de la guía codificada como "CCN-STIC-570A". A continuación, pulse el botón "Aceptar".  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.
30.	Pulse con botón derecho sobre la unidad organizativa "Domain Controllers" y seleccione "Crear un GPO en este dominio y vincularlo aquí…". 

Paso	Descripción
31.	Introduzca el nombre "CCN-STIC-576 incremental Controladores de Dominio Exchange categoria alta - DL" y pulse "Aceptar". 
32.	Seleccione la GPO recién creada y pulse "Editar…". 
33.	Despliegue el nodo **"Directiva CCN-STIC-576 ENS incremental Controladores de Dominio Exchange categoria alta - DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"** y haga doble clic sobre la directiva "Administrar registro de seguridad y auditoría". 

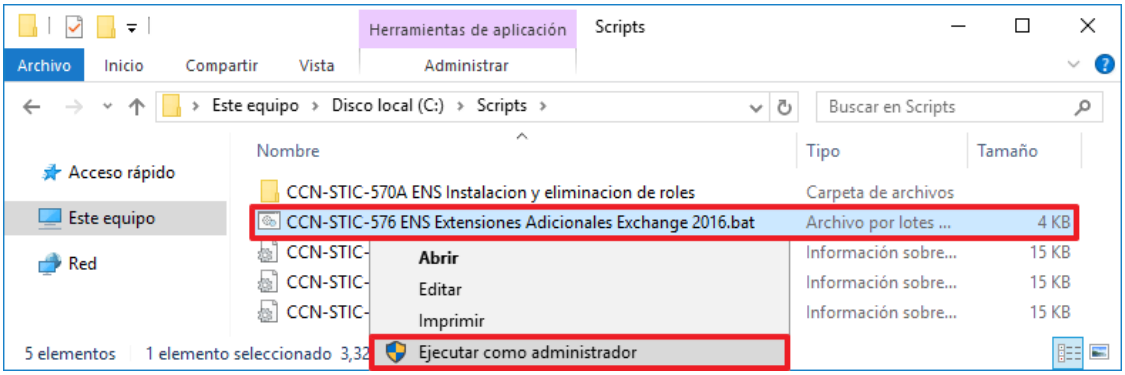
Paso	Descripción
34.	Marque la casilla "Definir esta configuración de directiva:" y pulse sobre "Agregar usuario o grupo…". 
35.	Pulse sobre "Examinar". 
36.	Añada los grupos "Administradores" y "Exchange Servers". Pulse "Aceptar". 

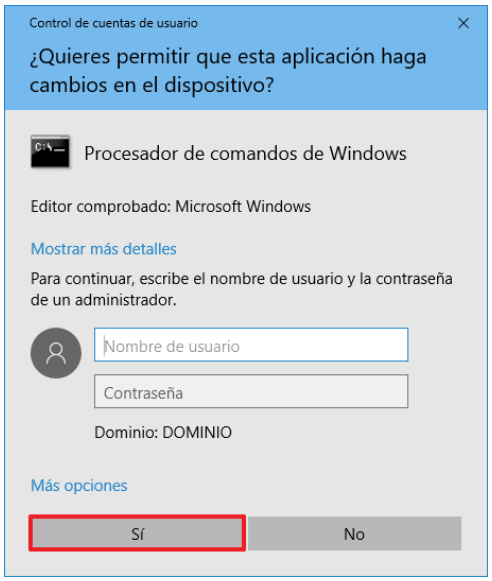
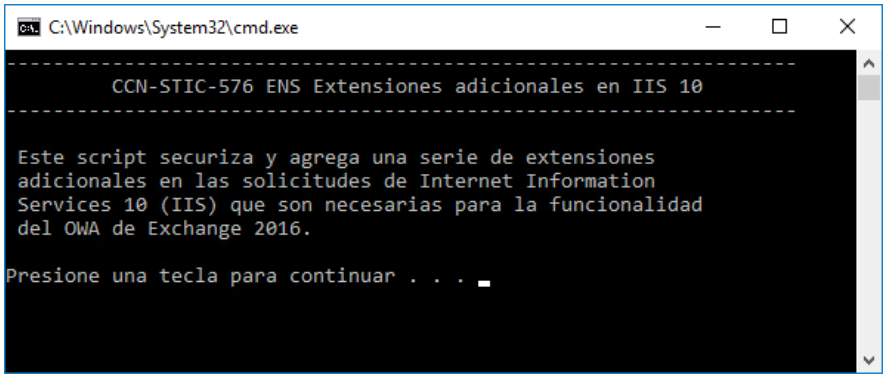
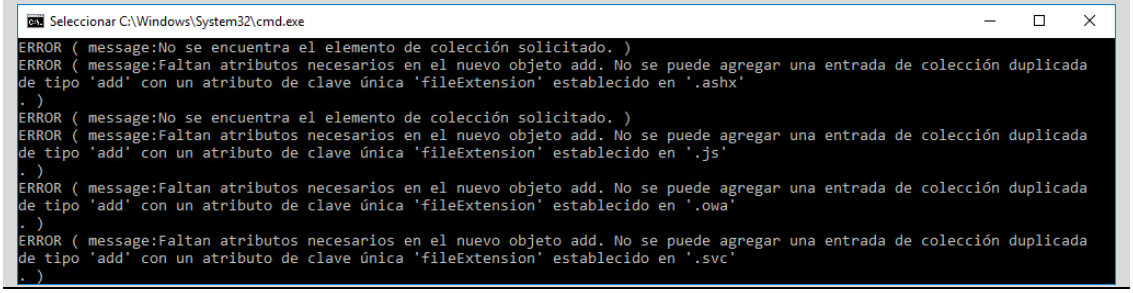
Paso	Descripción
37.	Pulse nuevamente sobre "Aceptar". 
38.	Para finalizar pulse sobre "Aplicar" y "Aceptar". 
39.	El protocolo de autenticación NTLM ha sido considerado inseguro por Microsoft y recomienda que no sea utilizado en entornos de dominio donde se requieren medidas de seguridad de nivel alto. Siguiendo esta recomendación, la guía de seguridad CCN-STIC-570A deshabilita completamente cualquier tipo de autenticación NTLM en todo el dominio, estableciendo la directiva incremental de dominio "Seguridad de red: restringir NTLM: autenticación NTLM en este dominio" en la opción "Denegar todo". Sin embargo, en ciertas situaciones, no es posible eliminar completamente el protocolo de autenticación NTLM ya que, incluso hoy en día, todavía algunos servicios de Microsoft requieren disponer de autenticación NTLM, como es el caso de Exchange Server 2016. Por este motivo se añade dicha directiva a la GPO del controlador del dominio y se incluye en la configuración de seguridad de la GPO incremental que aplica a los servidores Exchange, permitiendo el uso de dicho protocolo. En los próximos pasos se explica el procedimiento para realizarlo.

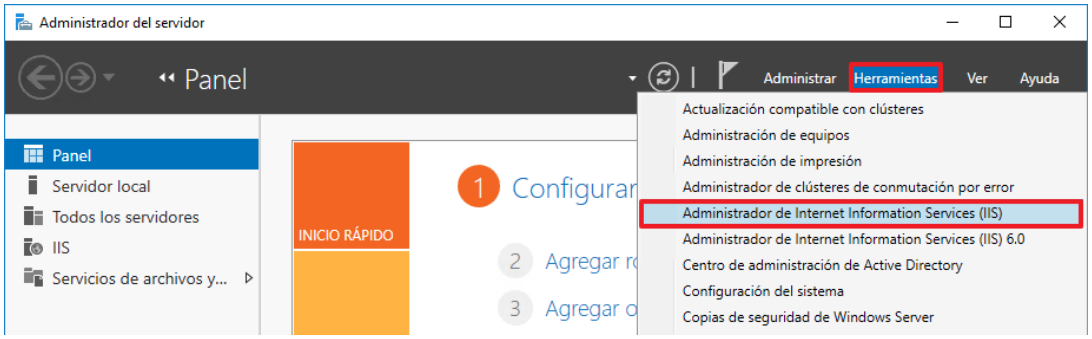
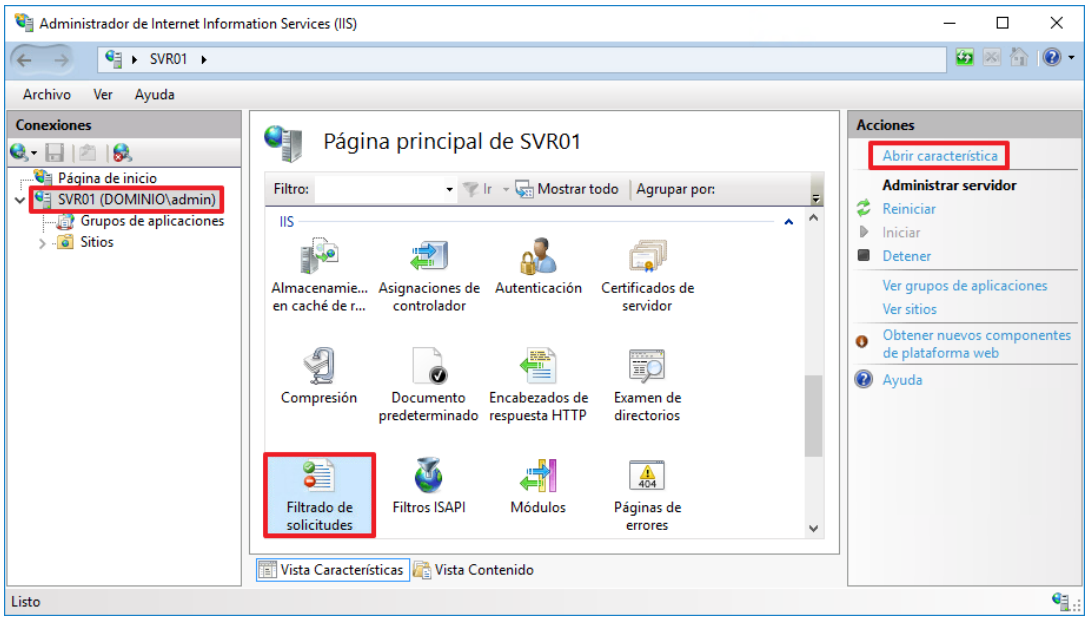
Paso	Descripción
40.	Despliegue el nodo **"Directiva CCN-STIC-576 ENS incremental Controladores de Dominio Exchange categoria alta - DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"** y haga doble clic sobre la directiva "Seguridad de red: restringir NTLM: autenticación NTLM en este dominio". 
41.	Marque la casilla "Definir esta configuración de directiva", establezca la opción en "Deshabilitar" y pulse "Aceptar". 
42.	Cierre todas las ventanas de administración y borre la carpeta "C:\Scripts".
43.	Reinicie los servidores para que se hagan efectivos los cambios.

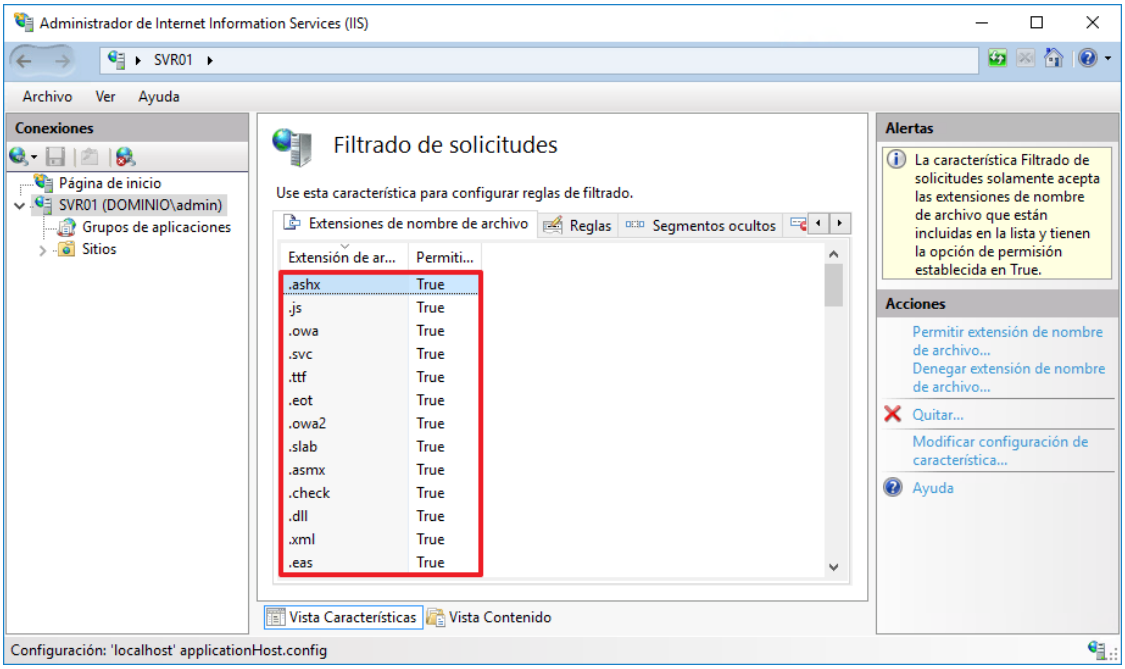
2. PREPARACIÓN DEL IIS 10

Los pasos que se describen a continuación se realizarán en un servidor miembro del dominio al que va a pertenecer el servidor Exchange Server 2016.

Paso	Descripción
44.	Inicie sesión en el servidor miembro donde tenga instalado IIS 10 para agregar las extensiones necesarias para el funcionamiento correcto de Exchange Server 2016.  **Nota:** Deberá iniciar sesión con una cuenta que sea "Administrador del Dominio".
45.	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, tendría que editar los scripts para reflejar la nueva ubicación.
46.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".
47.	Se debe ejecutar el script que permite agregar extensiones al servidor IIS 10. Por lo tanto, con el botón derecho seleccione el fichero denominado "CCN-STIC-576 ENS Extensiones adicionales Exchange 2016.bat" y seleccione "Ejecutar como administrador". 

Paso	Descripción
48.	El control de cuentas de usuario le solicitará las credenciales de un usuario con permisos de administrador de dominio. 
49.	Aparecerá la siguiente pantalla. Pulse una tecla para continuar.  **Nota:** Si tras la ejecución del script aparece un mensaje de error advirtiendo de que no se puede agregar una entrada de colección duplicada, significa que este procedimiento se ha realizado anteriormente. Omita dicho error y continúe con la ejecución del siguiente paso. 
50.	Cuando haya finalizado la ejecución, pulse una tecla para cerrar la ventana.

Paso	Descripción
51.	Compruebe que se ha aplicado correctamente la configuración de las extensiones, para ello, diríjase al administrador de IIS dentro del desplegable "Herramientas" del "Administrador del servidor". 
52.	Compruebe que se ha aplicado correctamente la configuración de las extensiones, para ello, diríjase al administrador de IIS, seleccione la opción "Filtrado de solicitudes" y en el menú situado en el lateral derecho, pulse "Abrir característica". 

Paso	Descripción
53.	Compruebe que las extensiones de nombre de archivo específicas para Exchange Server 2016 están configuradas correctamente en la columna "Permitido" en "True". Para ello diríjase a la pestaña "Extensiones de nombre de archivo". – .ashx – .js – .owa – .svc – .ttf – .eot – .owa2 – .slab – .asmx – .check – .dll – .eas  **Nota:** En caso de que no aparezca reflejada alguna de las extensiones de nombre de archivo arriba referenciadas, deberá crearlas a mano a través del menú "Acciones" situado a la derecha.
54.	Una vez realizada la comprobación cierre el administrador de Internet Information Services.

3. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

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

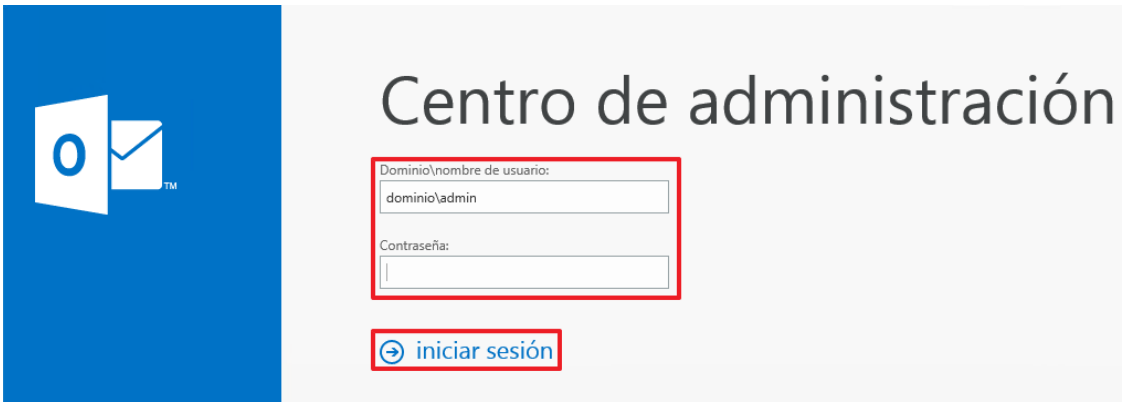
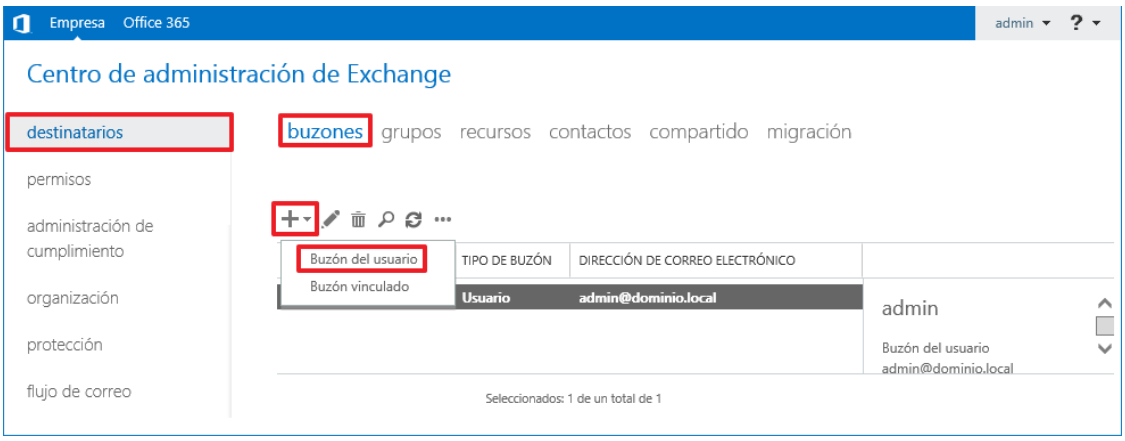
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

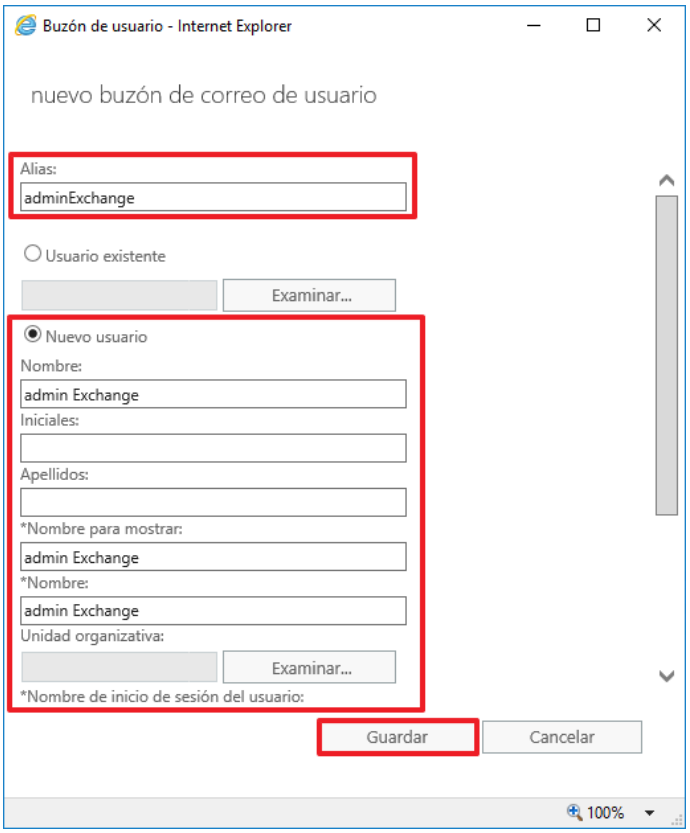
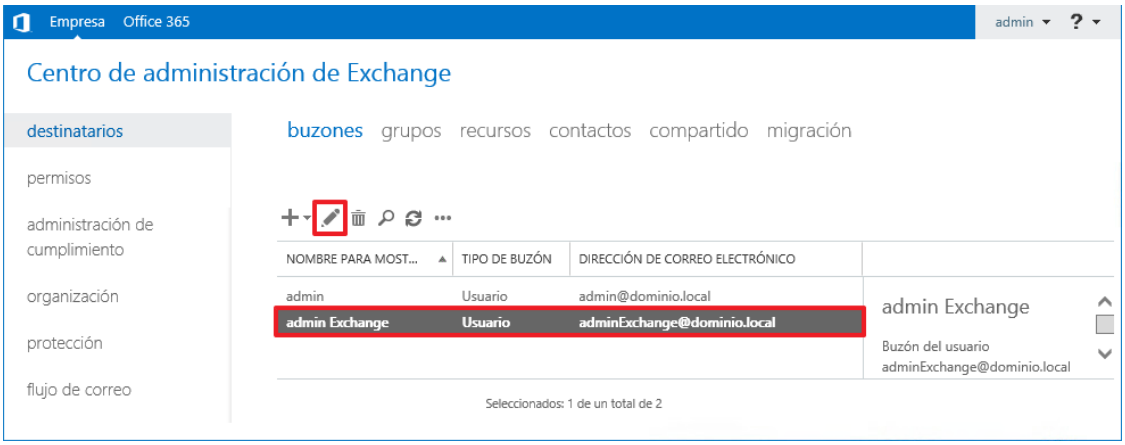
Nota: Todas las recomendaciones de seguridad indicadas en la presente guía deben ser adaptadas al entorno de su organización. Se aconseja realizar las pruebas pertinentes en un entorno de preproducción antes de ser incluidas en su entorno de producción.

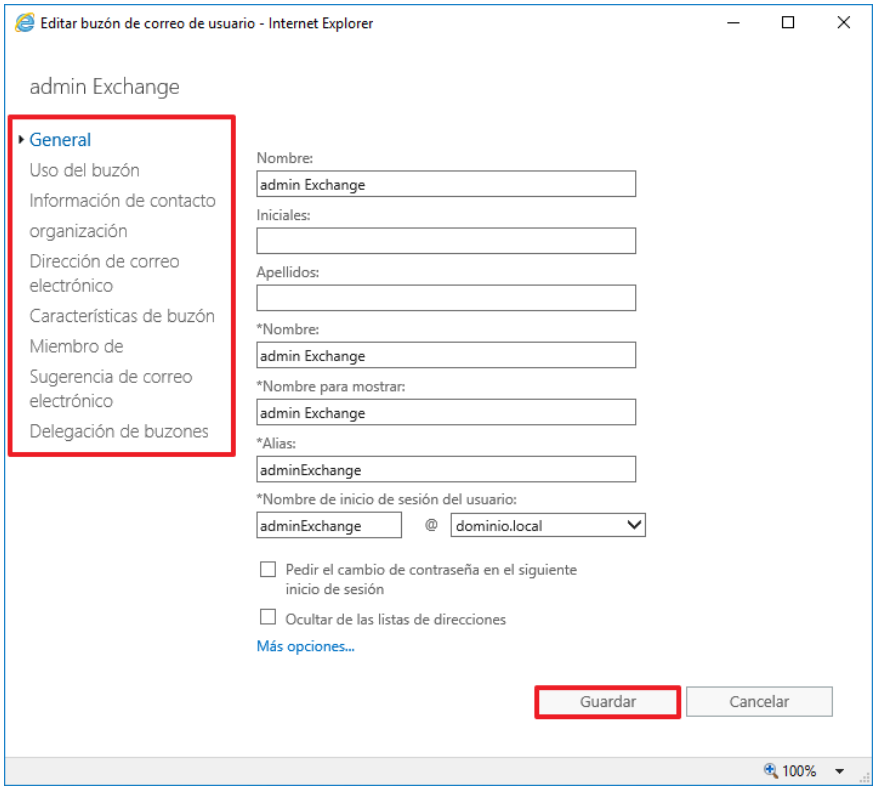
3.1. IDENTIFICACIÓN

Es recomendable que los accesos a los buzones estén completamente controlados y registrados, por ello se deberá usar el directorio activo para la creación de usuarios. Exchange Server 2016 facilita la creación de usuarios de directorio activo integrando en su propio panel de administración toda la creación y gestión del usuario sincronizándose automáticamente con el directorio activo de su organización.

Paso	Descripción
55.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
56.	Pulse sobre "Internet Explorer" en la barra de tareas. 

Paso	Descripción
57.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.
58.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
59.	Seleccione en la pestaña "destinatarios" en la opción de "buzones" un nuevo "Buzón del usuario". 

Paso	Descripción
60.	A continuación, documente los datos del nuevo buzón que desea crear, una vez documentado pulse sobre "Guardar".  **Nota:** También se pueden crear un buzón a un usuario existente en el directorio activo, en este ejemplo se crea un usuario nuevo con su correspondiente buzón.
61.	Una vez creado el nuevo usuario y buzón es posible modificar más características editándolo. Para ello seleccione el buzón que desea editar y pulse "Modificar". 

Paso	Descripción
62.	En la siguiente pantalla puede añadir todos los datos adicionales necesarios para su organización, para ello debe navegar por las diferentes opciones situados en el panel izquierdo. Para finalizar pulse sobre "Guardar". 

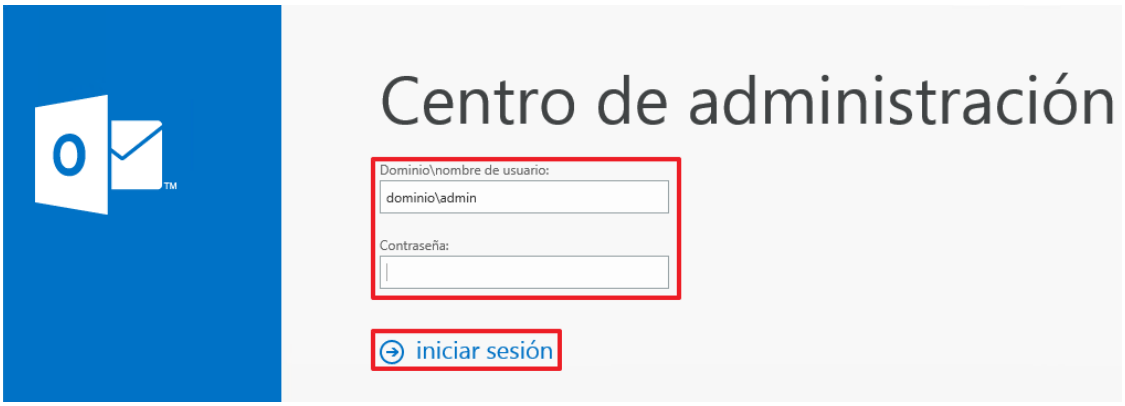
3.2. ASIGNACIÓN DE PERMISOS Y ROLES

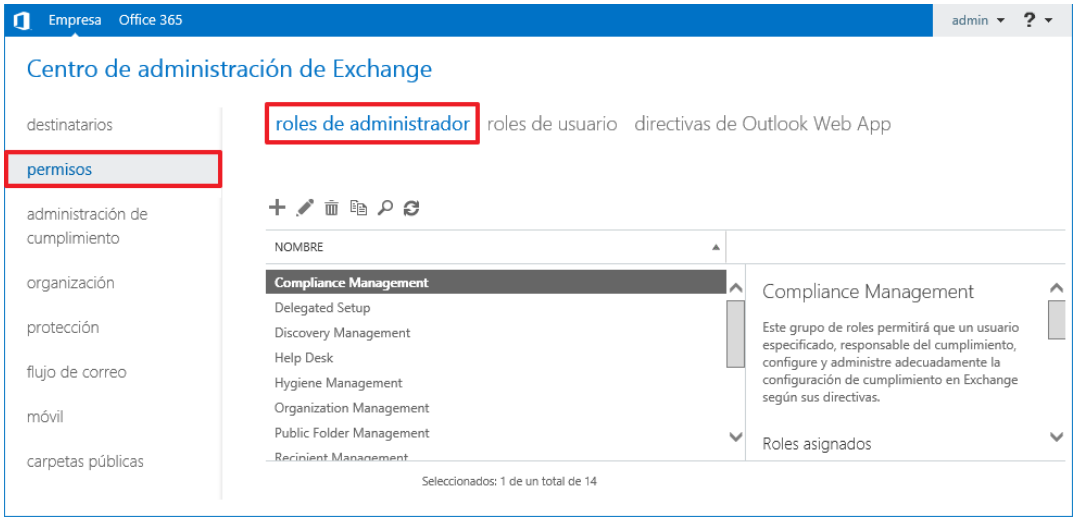
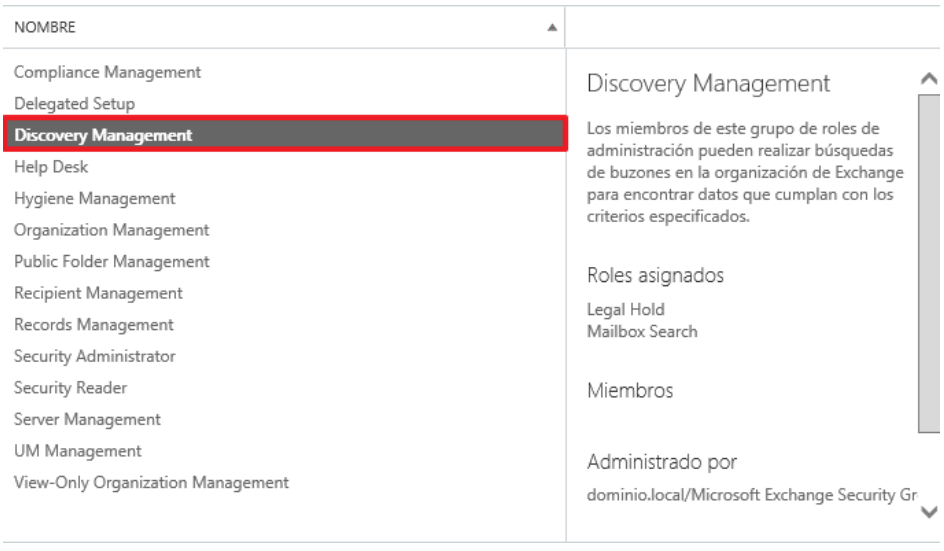
Antes de poder aplicar diferentes mecanismos de auditoría y conformidad, debe tener presente que determinadas funcionalidades requieren de la obtención de permisos específicos para la realización de las operaciones. La asignación de dichos permisos se basa en el modelo RBAC (Role Based Access Control). Dicho modelo tiene su base fundamental en la pertenencia a grupos y a la aplicación de directivas sobre dichos grupos.

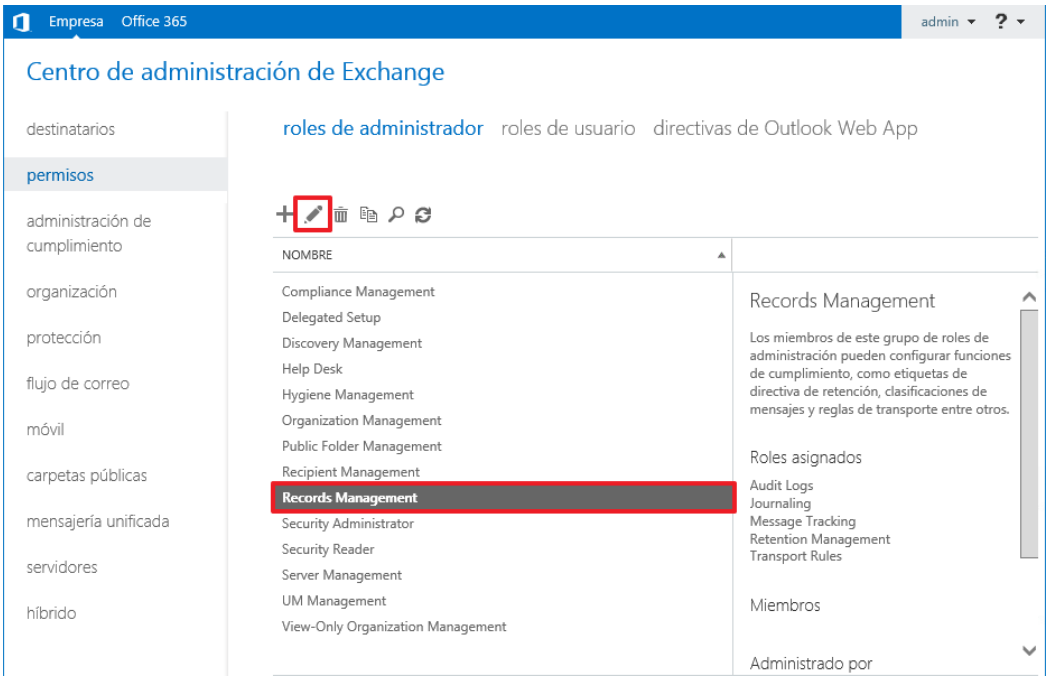
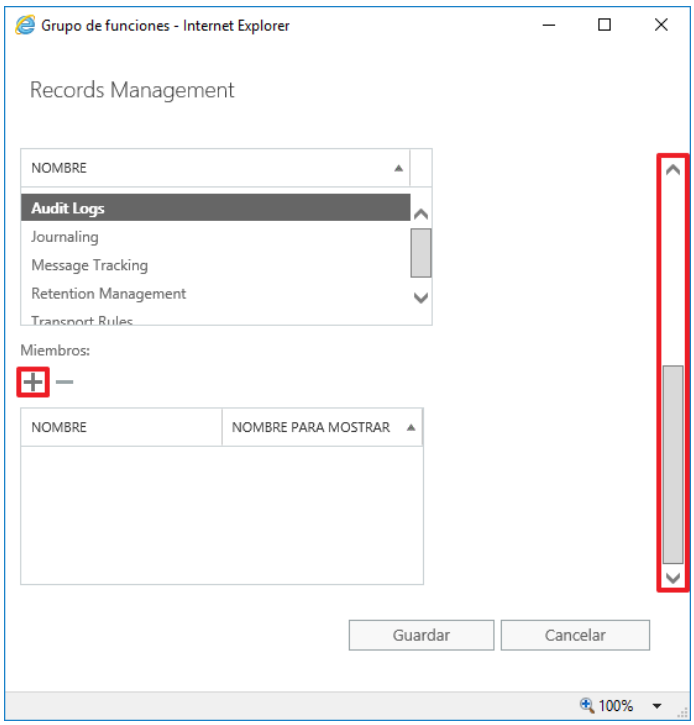
Así mismo, este modelo permite establecer una jerarquía de roles segregados, de tal forma que algunos usuarios de la organización pueden realizar tareas de administración del servidor, a la vez que otros pueden asumir la funcionalidad de auditores del sistema.

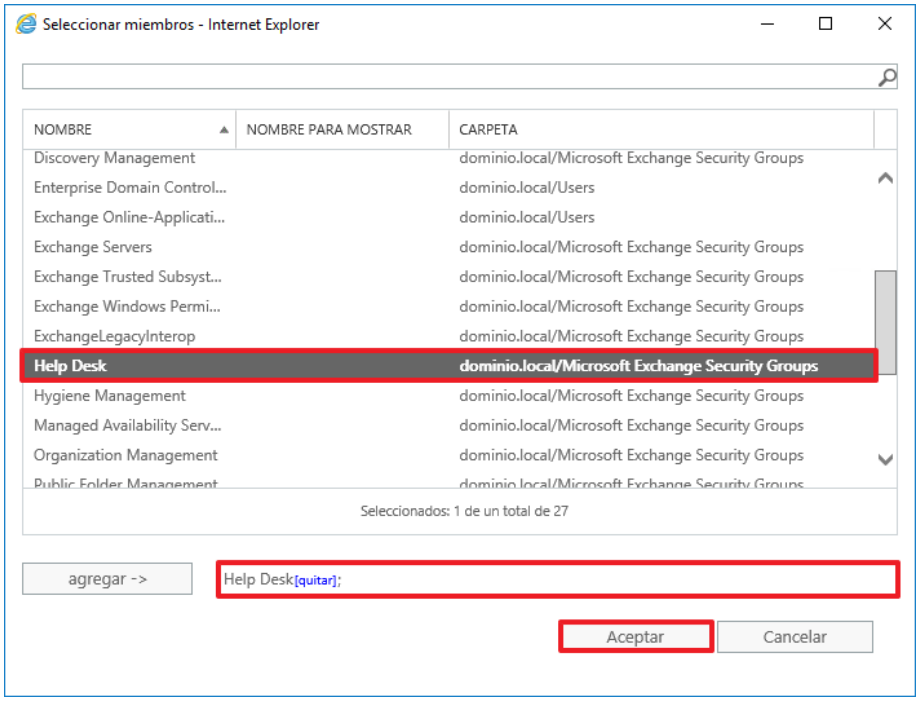
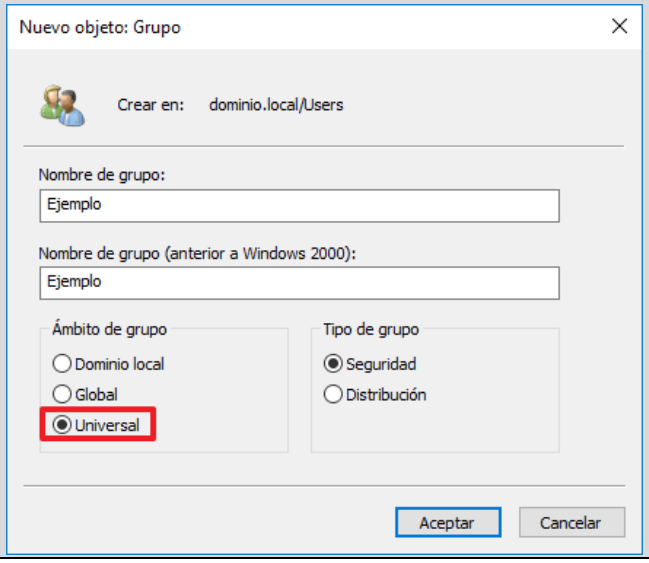
La administración de roles y permisos se puede realizar a través de la consola Web de administración (Exchange Control Panel) o bien a través de cmdlets de PowerShell. Para una mejor comprensión, este anexo mostrará cómo realizar dichas acciones a través del entorno gráfico vía Web.

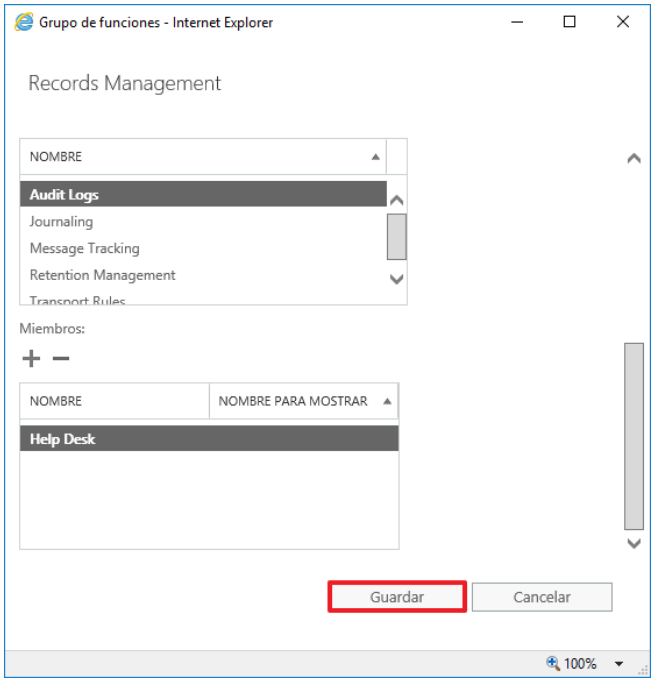
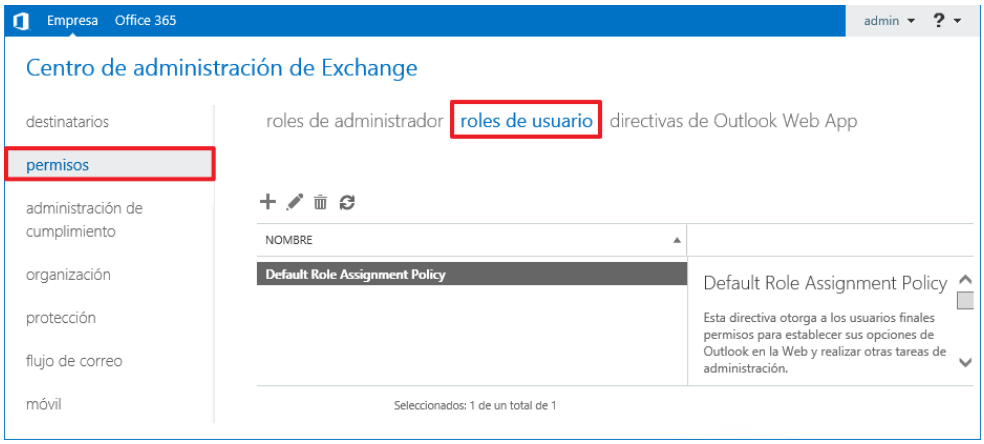
Nota: Si desea crear más información sobre la administración de roles y permisos visite la siguiente web: https://technet.microsoft.com/es-es/library/jj657511(v=exchg.150).aspx.

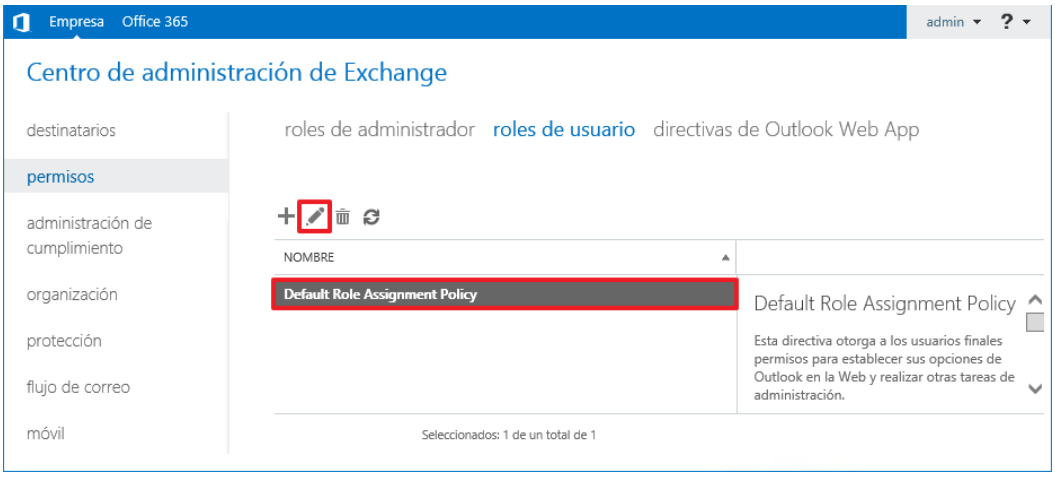
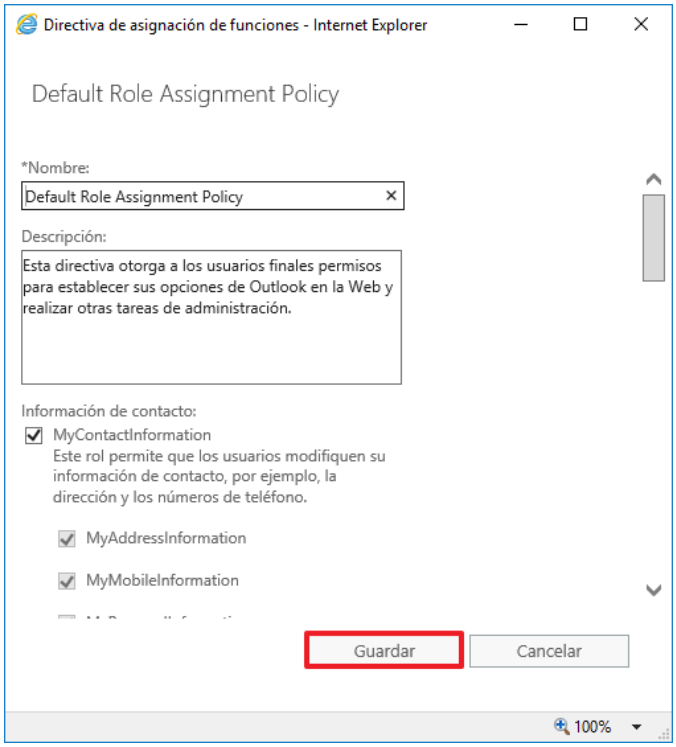
Paso	Descripción
63.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
64.	Pulse sobre "Internet Explorer" en la barra de tareas. 
65.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.
66.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".

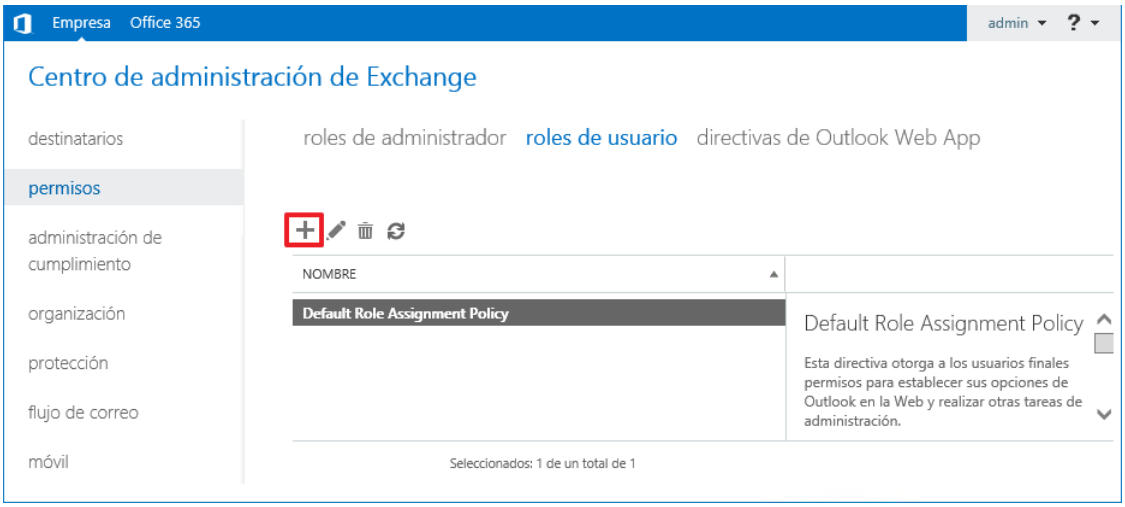
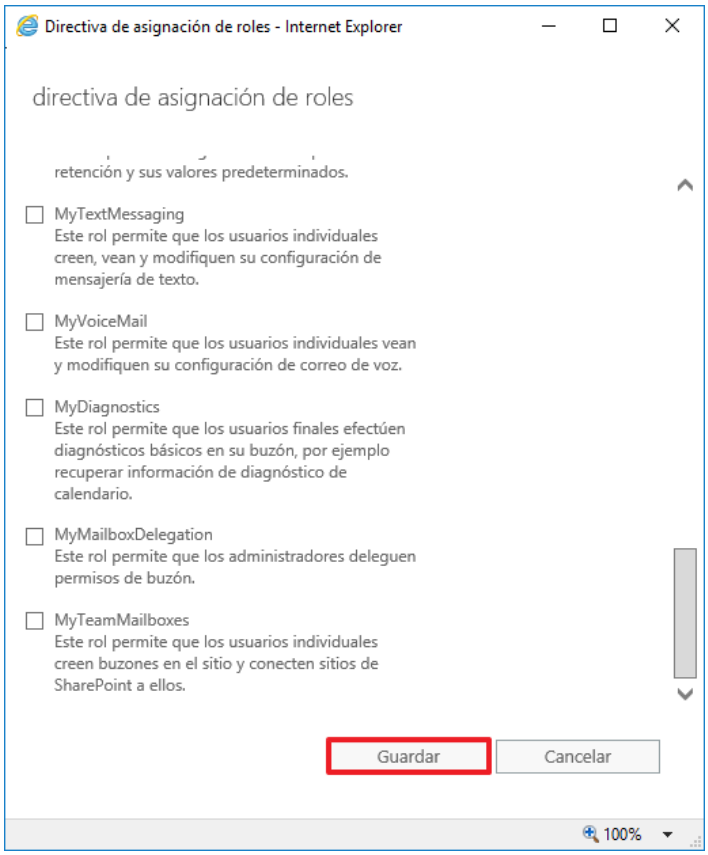
Paso	Descripción
67.	Seleccione el enlace "Permisos" para configurar los permisos RBAC.  **Nota:** Desde este menú se pueden asignar roles de administrador predeterminados a grupos nuevos o existentes en la organización, o también se pueden crear nuevos roles de administrador con permisos específicos.
68.	Por ejemplo, el rol denominado "Discovery Management" o administración de la detección tiene asignados los permisos necesarios para trabajar con la retención legal, así como la suspensión y exhibición de datos electrónicos. Estos permisos incluyen la realización de búsquedas de buzones en la organización para obtener datos que cumplan determinados criterios y la configuración de retenciones legales en los diferentes buzones de correo. 

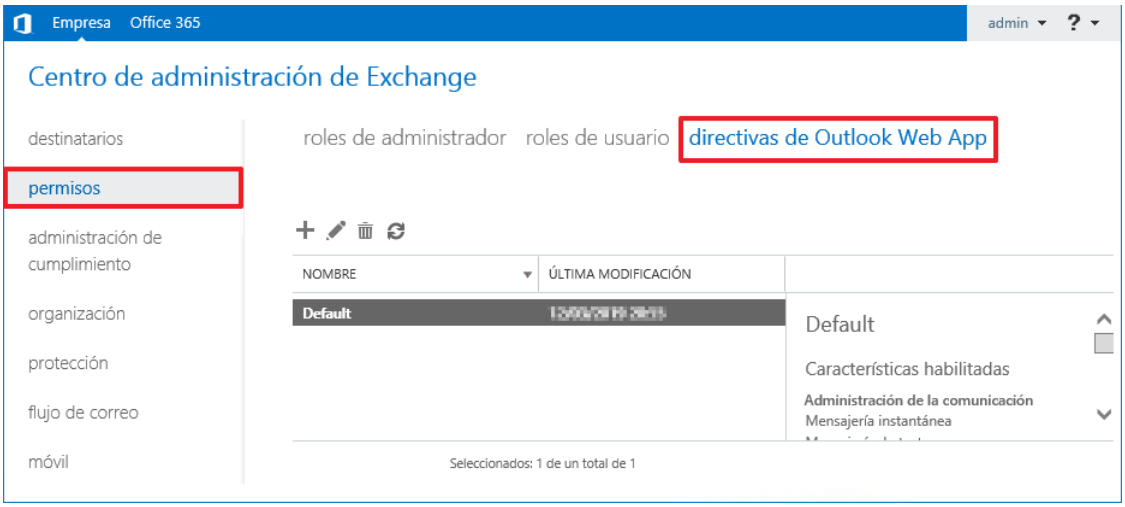
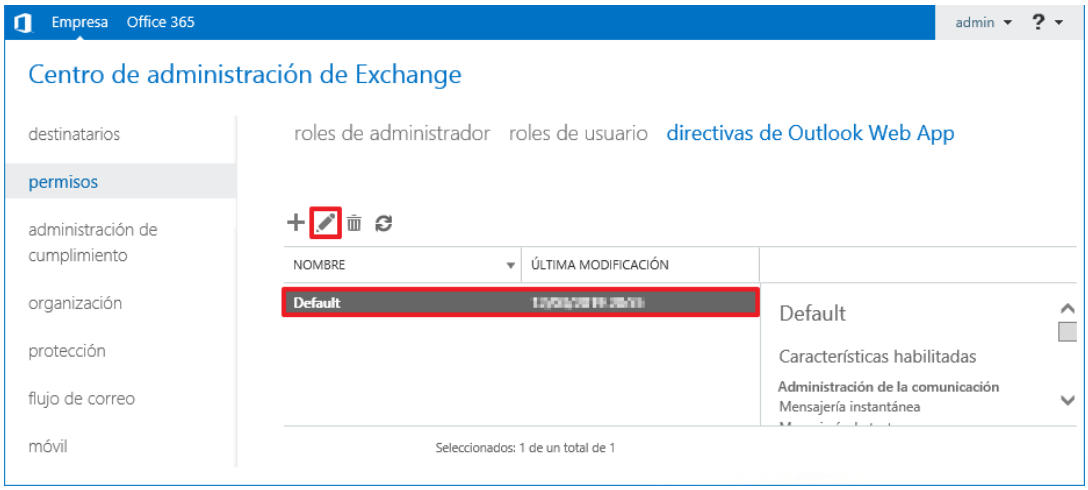
Paso	Descripción
69.	Por otro lado, el rol denominado "Records Management" o administración de registros, incluye otra serie de permisos asignados relativos a las capacidades de auditoría. A continuación, a modo de ejemplo, se va a asignar dicho rol a un grupo de seguridad de Directorio Activo. Para ello, seleccione el rol "Records Management" y pulse el botón "Modificar". 
70.	A continuación, en la sección "Miembros", podrá agregar un grupo de seguridad de Directorio Activo pulsando en el botón "+". 

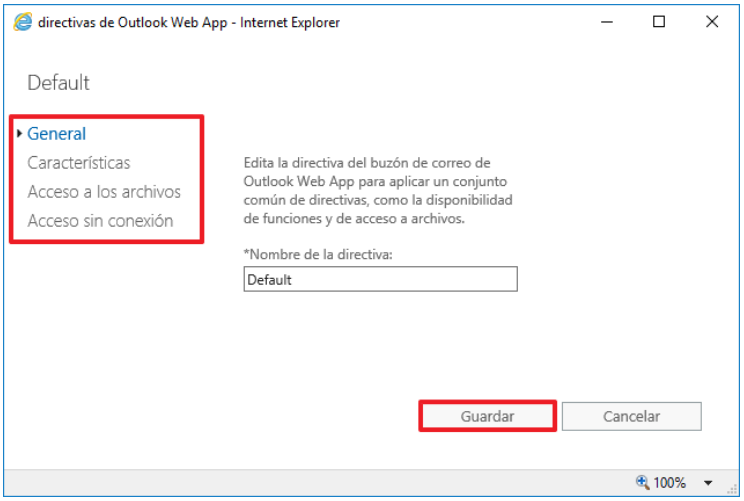
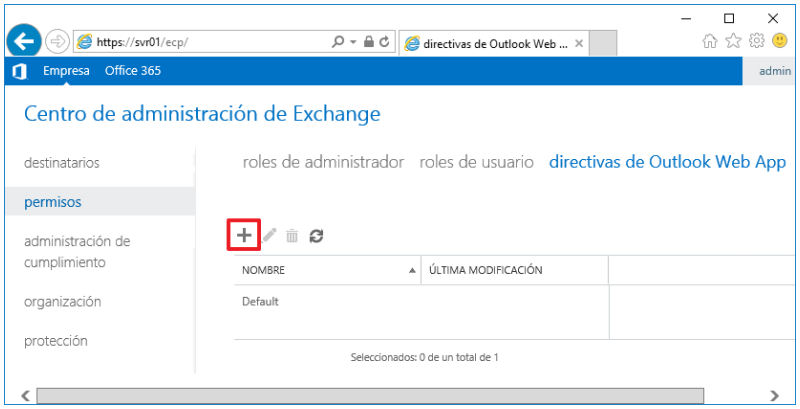
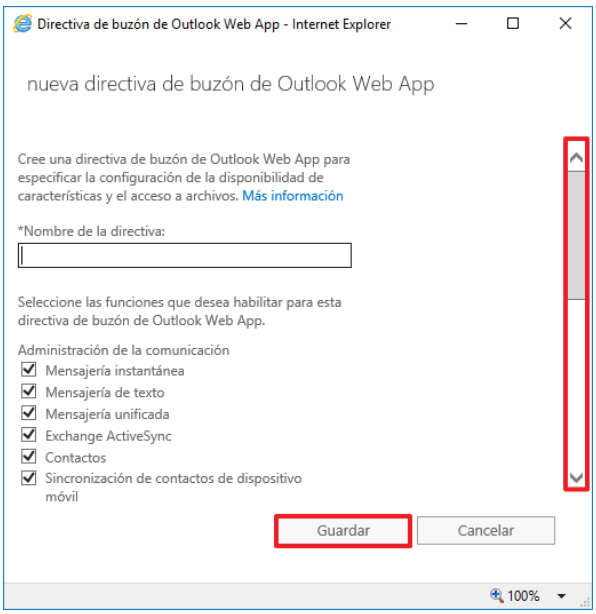
Paso	Descripción
71.	En la pantalla de selección, localice las cuentas de usuarios o grupos de seguridad universales que se desean añadir y pulse el botón "Agregar". Por ejemplo, seleccione el grupo "Help Desk" y pulse en el botón "agregar" y "aceptar".  **Nota:** Para que los grupos de seguridad del Directorio Activo aparezcan en esta ventana de selección, deben ser grupos universales. Los grupos globales o locales no serán visibles. 

Paso	Descripción
72.	A continuación, pulse sobre el botón "Guardar" para hacer efectivos los cambios. 
73.	A continuación, también puede crear grupos de roles de usuario para ello diríjase a la pestaña "permisos" y después a la pestaña "roles de usuario". 

Paso	Descripción
74.	Es posible modificar el grupo de roles de usuario por defecto, pulse sobre el grupo "Default Role Assignment Policy" y a continuación, seleccione "Modificar". 
75.	A continuación, se pueden modificar los campos que sean necesarios para adaptarlos a los requerimientos de su organización y pulse "Guardar". 

Paso	Descripción
76.	Del mismo modo es posible crear un grupo de roles de usuario nuevo, para ello seleccione la pestaña "roles de usuario" pulse sobre la opción nuevo o "+". 
77.	A continuación, cumplimente los campos en función de las necesidades de su organización y pulse "Guardar". 

Paso	Descripción
78.	Del mismo modo puede cambiar las directivas de Outlook Web App, para ello diríjase a la opción "directivas de Outlook Web App". 
79.	A continuación, seleccione la opción que viene creada por defecto, para ello seleccione "Default" y pulse el icono "Modificar".  **Nota:** El valor predeterminado de directiva de buzón de correo de Outlook Web App tiene todas las opciones habilitadas de forma predeterminada.

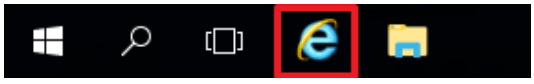
Paso	Descripción
80.	A continuación, cumplimente los campos en función de las necesidades de su organización y pulse "Guardar". 
81.	Si desea crear un grupo de directivas nuevo, debe pulsar sobre nuevo o "+". 
82.	Rellene los campos en función de las necesidades de su organización y pulse "Guardar". 

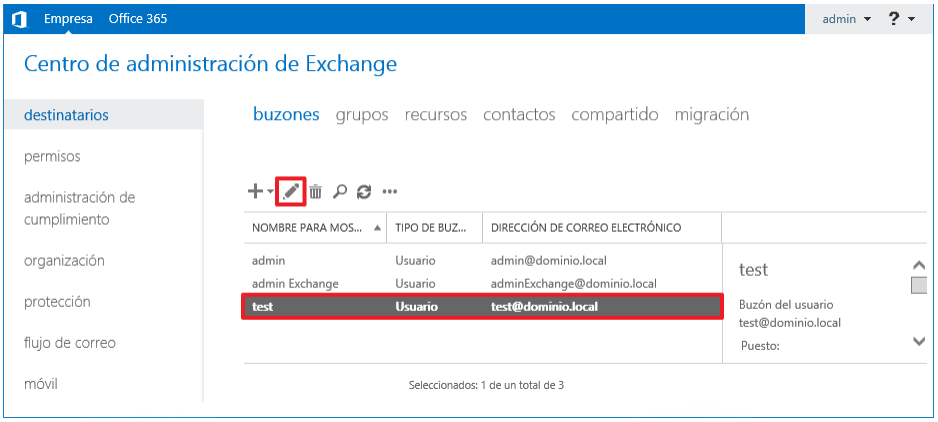
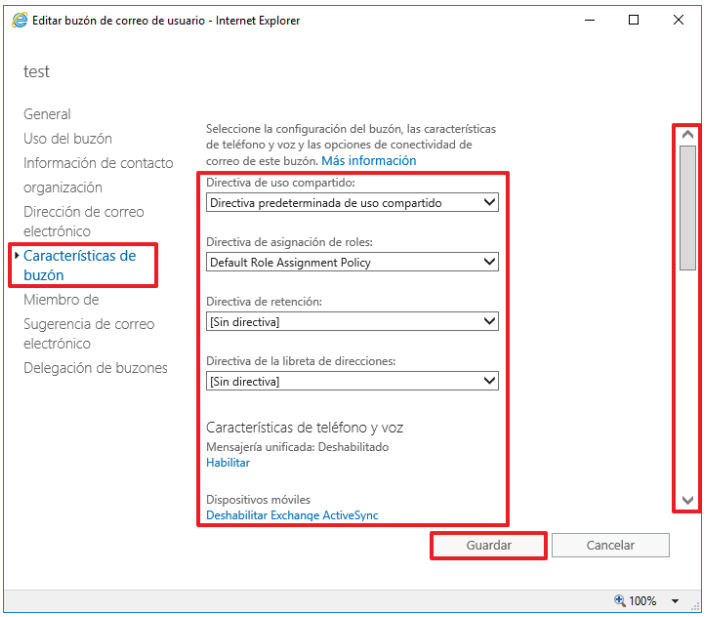
3.3. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

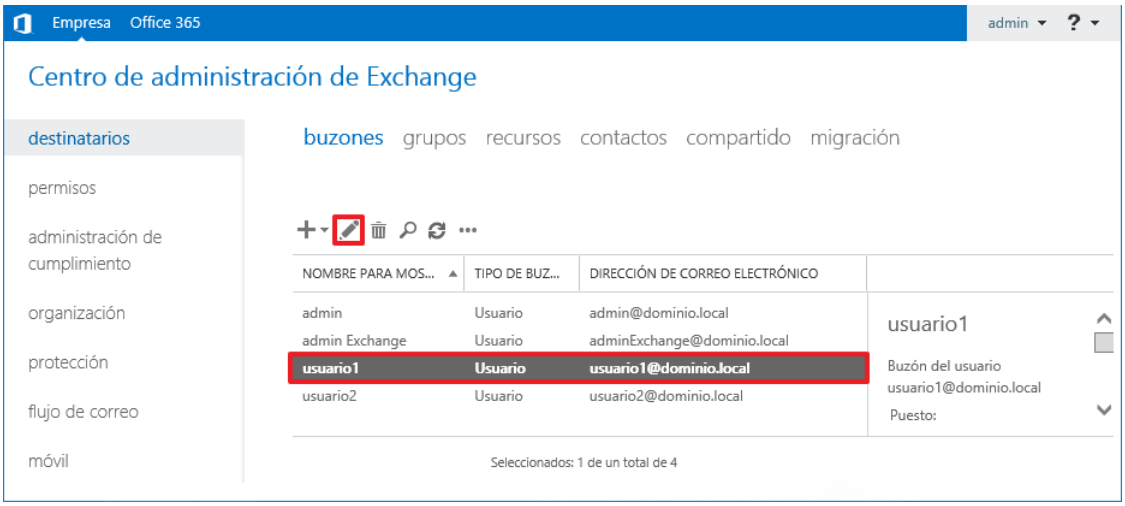
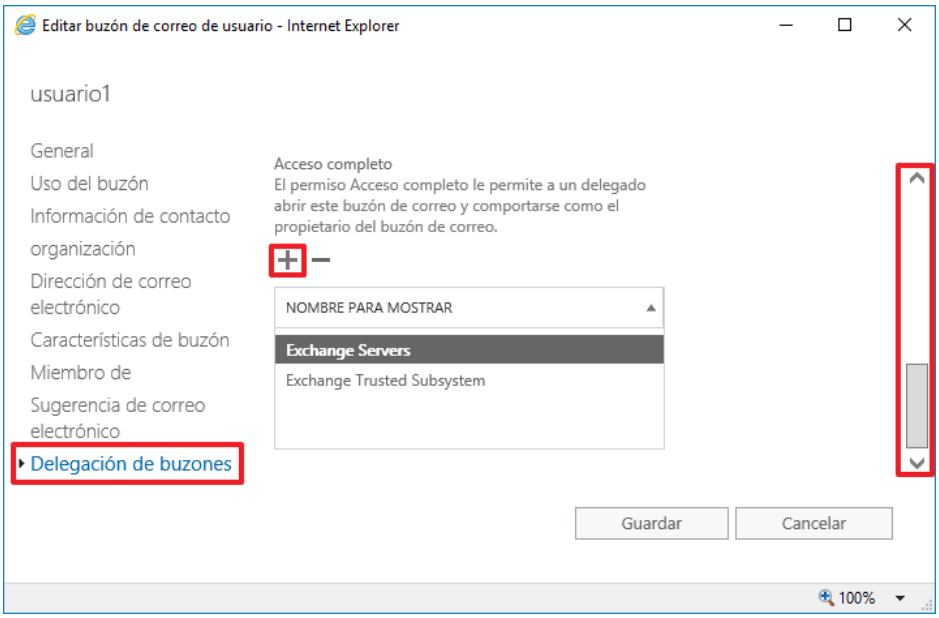
Uno de los aspectos que marca el ENS, desde su requisito de categoría alta - DL en el Marco Operacional, es la mínima funcionalidad y mínima exposición evitando con ello posibles vulnerabilidades minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida 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.

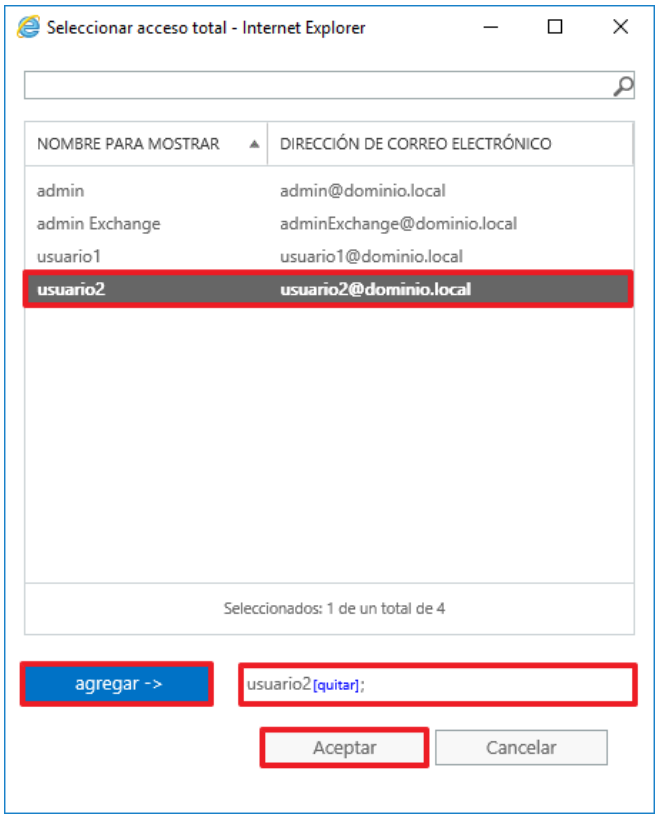
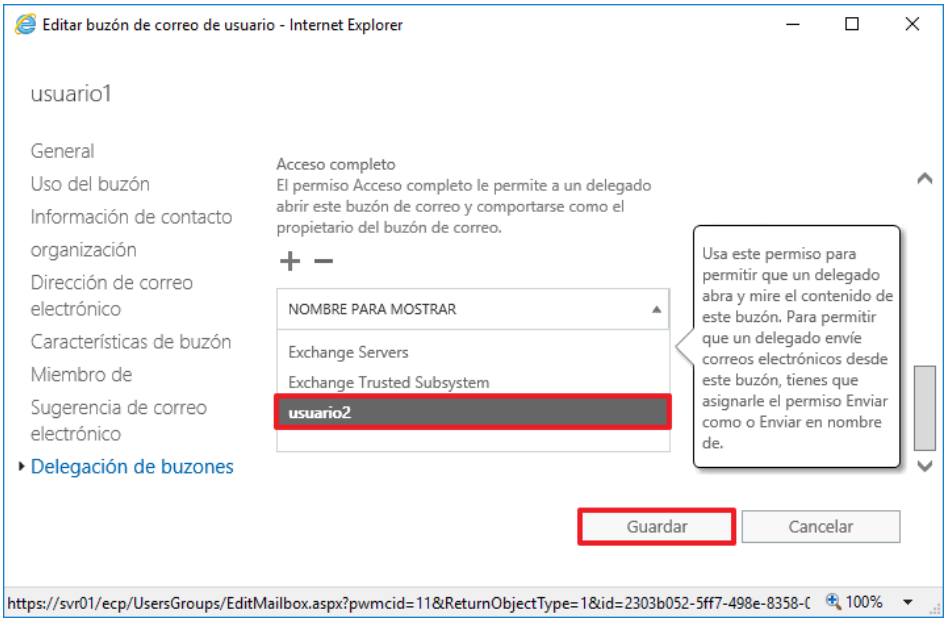
Microsoft Exchange Server 2016 instala por defecto las mínimas funcionalidades para el uso correcto de su producto, por lo que no es posible desinstalar características ya que conllevaría un mal funcionamiento del producto.

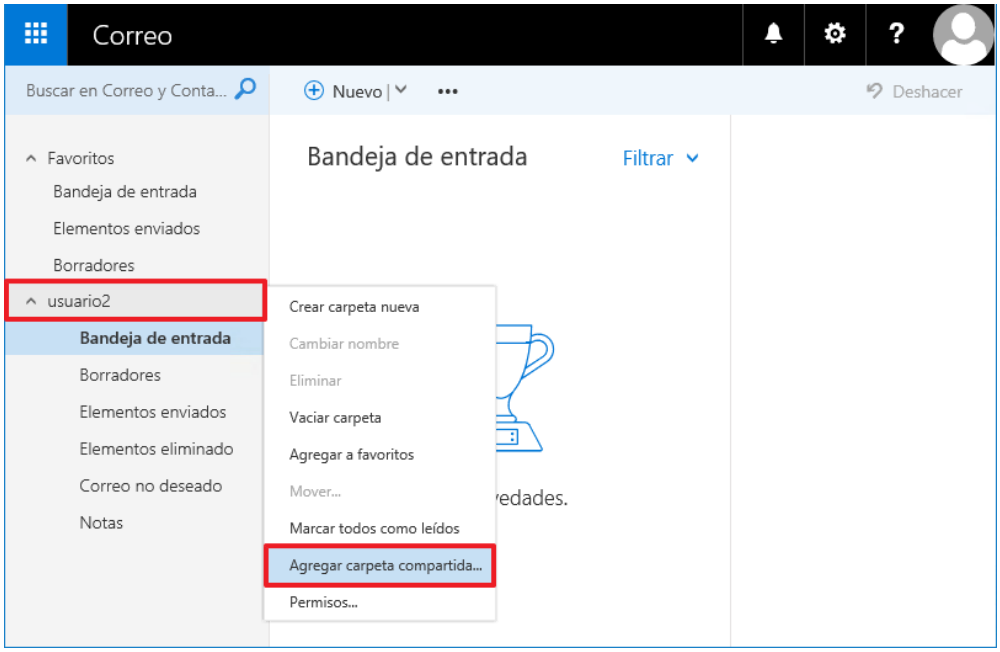
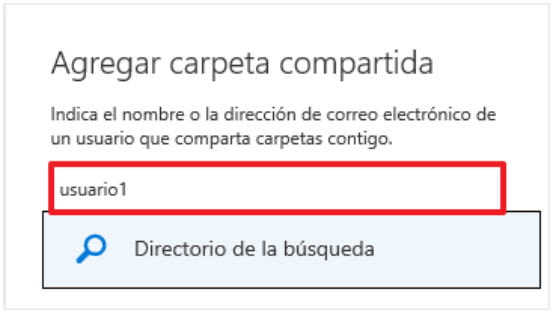
Microsoft Exchange Server 2016 por defecto deshabilita diferentes funcionalidades para aplicar seguridad en el entorno, por ejemplo, los servicios de POP3 e IMAP vienen deshabilitados por lo que si es necesario para su entorno deberá habilitarlo manualmente.

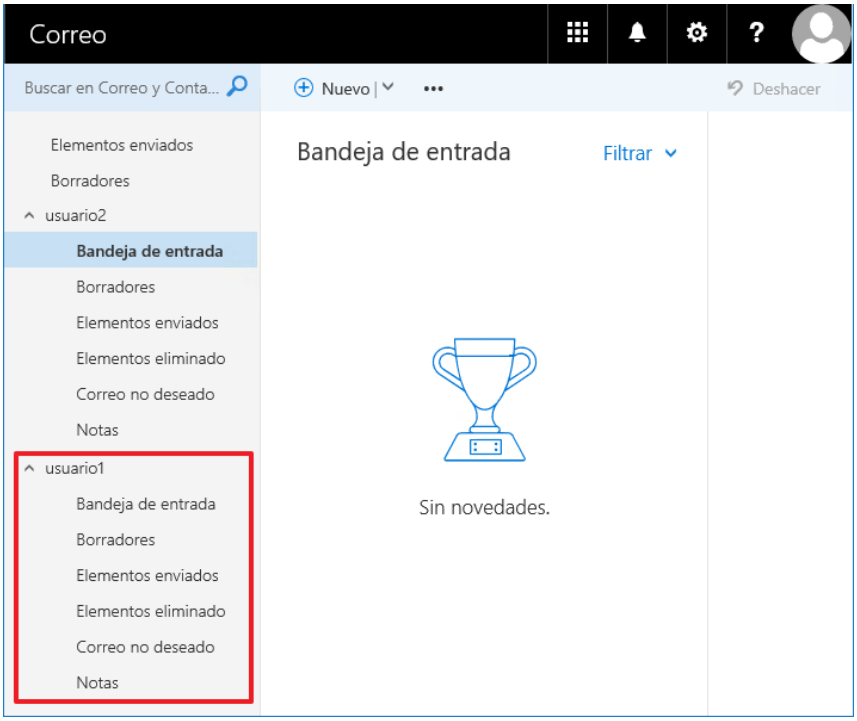
Paso	Descripción
83.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
84.	Pulse sobre "Internet Explorer" en la barra de tareas. 
85.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.

Paso	Descripción
86.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
87.	Seleccione el usuario o buzón en el que desea modificar alguna de las funcionalidades editándolo. Para ello seleccione el buzón que desea editar y pulse "Modificar".  **Nota:** En este ejemplo se usa la cuenta "test". Deberá adaptar los pasos de acuerdo a las necesidades de su organización.
88.	Localice en el menú lateral izquierdo, la opción de "Características de buzón" y seleccione la configuración de buzón según las necesidades de su organización. 

Paso	Descripción
89.	Una característica de seguridad configurable es la posibilidad que un usuario tenga acceso a un buzón de otro usuario, para ello se debe primero conceder los permisos necesarios para acceder al buzón. Seleccione el buzón al que desea acceder con otro usuario y pulse editar.  **Nota:** Para poder realizar este ejemplo se han creado previamente dos buzones, usuario1 y usuario2.
90.	A continuación, desplácese hacia abajo hasta localizar la característica "Acceso completo" dentro del menú "Delegación de buzones" y pulse el botón "Agregar". 

Paso	Descripción
91.	Seleccione el usuario al que desea dar acceso al buzón, pulse "agregar ->" y "Aceptar". 
92.	Compruebe que se ha añadido al usuario dentro de "Acceso Completo". Para finalizar, pulse "Guardar". 

Paso	Descripción
93.	Para comprobar la correcta configuración, inicie sesión en el buzón del "Usuario2", pulse botón derecho sobre una carpeta, y seleccione "Agregar carpeta compartida...".  **Nota:** En este ejemplo se ha usado la cuenta de correo "Usuario2". Adapte estos pasos a los más convenientes para su organización.
94.	A continuación, escriba el usuario o el buzón que desee agregar. 
95.	Una vez seleccionado el usuario pulse "Agregar". 

Paso	Descripción
96.	Compruebe que tiene acceso al nuevo buzón agregado. 

3.4. MECANISMOS DE AUTENTICACIÓN

En Microsoft Exchange Server 2016 la autenticación básica establecida por defecto se realiza con usuario y contraseña gracias a la integración con el directorio activo de su organización asegurando que las contraseñas cumplan con los requisitos mínimos que se establecen en el ENS, por lo que se deben asegurar en la categoría alta - DL del marco operacional unas claves seguras.

En la categoría alta - DL del marco operacional del ENS se recomienda no usar claves concertadas, aunque si está permitido su uso.

En la categoría alta - DL del marco operacional del ENS se recomienda el uso de tarjetas inteligentes para el cual es necesario el uso del cifrado del nivel de sockets seguros (SSL), de manera predeterminada Outlook Web Access utiliza SSL por lo que si desea usar la autenticación mediante tarjeta inteligente deberá mantenerlo habilitado o habilitarlo en necesario, además deberá obtener y configurar un certificado de una entidad de certificación de confianza.

Nota: Si desea más información sobre cómo configurar Outlook Web Access para el uso de una tarjeta inteligente visite el siguiente sitio web: https://technet.microsoft.com/en-us/library/bb691090(v=exchg.80).aspx

3.5. CERTIFICADOS

Cuando se instala Microsoft Exchange Server 2016, se configura por defecto un certificado autofirmado en los servidores de buzones de correo. Este certificado autofirmado se usa para cifrar comunicaciones entre el servidor de acceso de cliente y el servidor de buzones de correo.

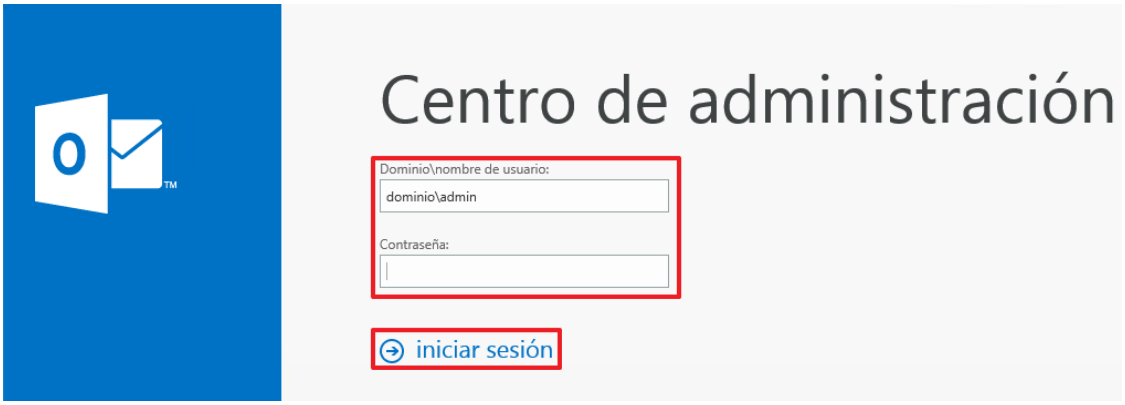
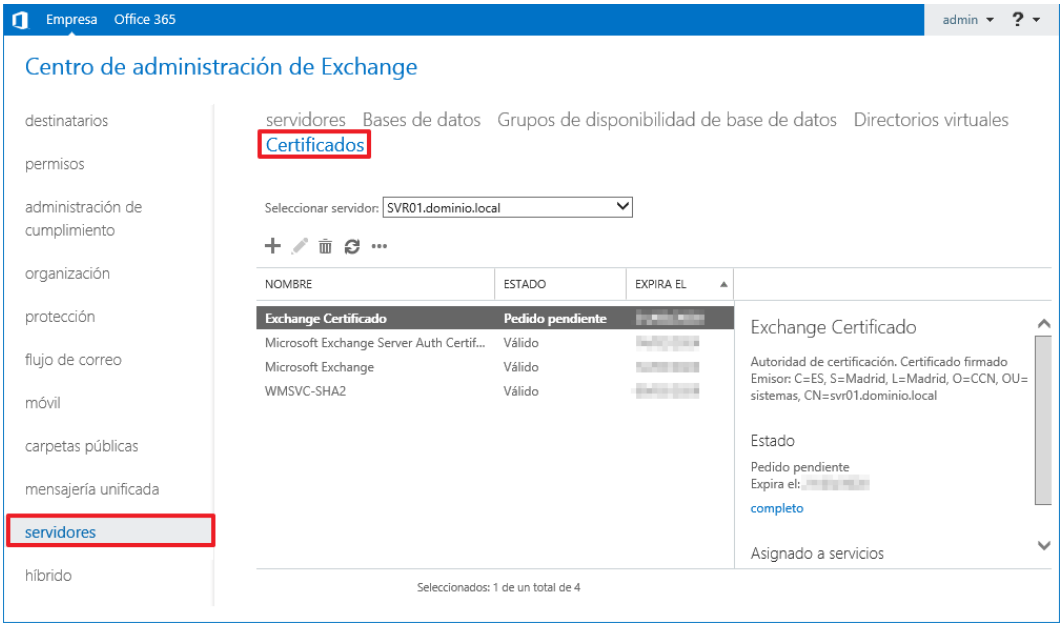
El servidor de acceso de cliente confía en el certificado autofirmado del servidor de buzones de correo automáticamente, así que no es necesario un certificado de terceros en el servidor de buzones de correo. Este certificado autofirmado permitirá que algunos protocolos de cliente usen SSL para sus comunicaciones. Exchange ActiveSync y Outlook Web App, pueden establecer una conexión SSL usando un certificado autofirmado.

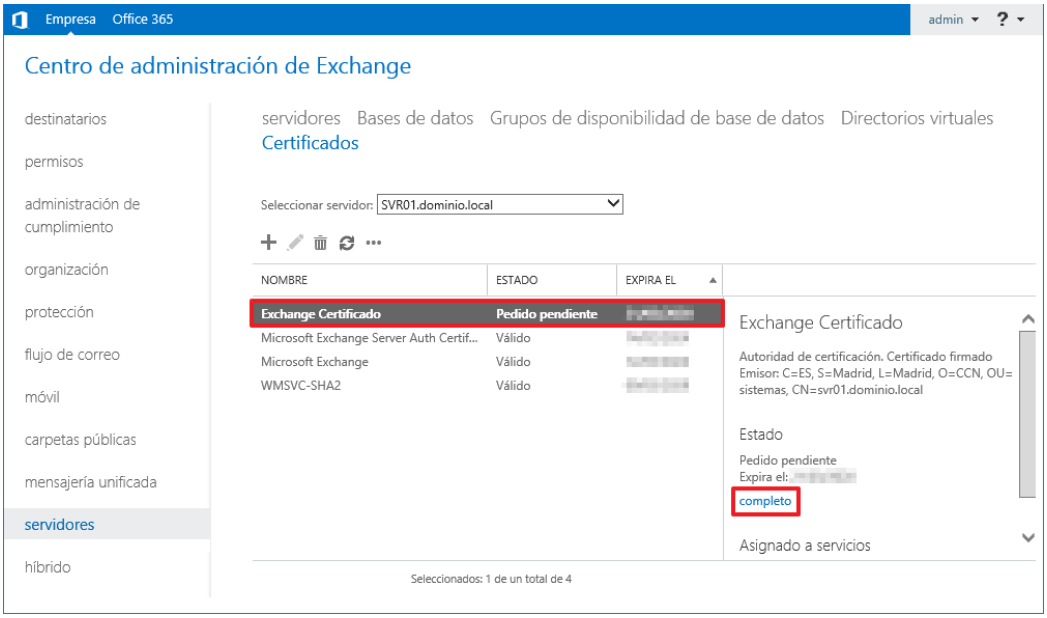
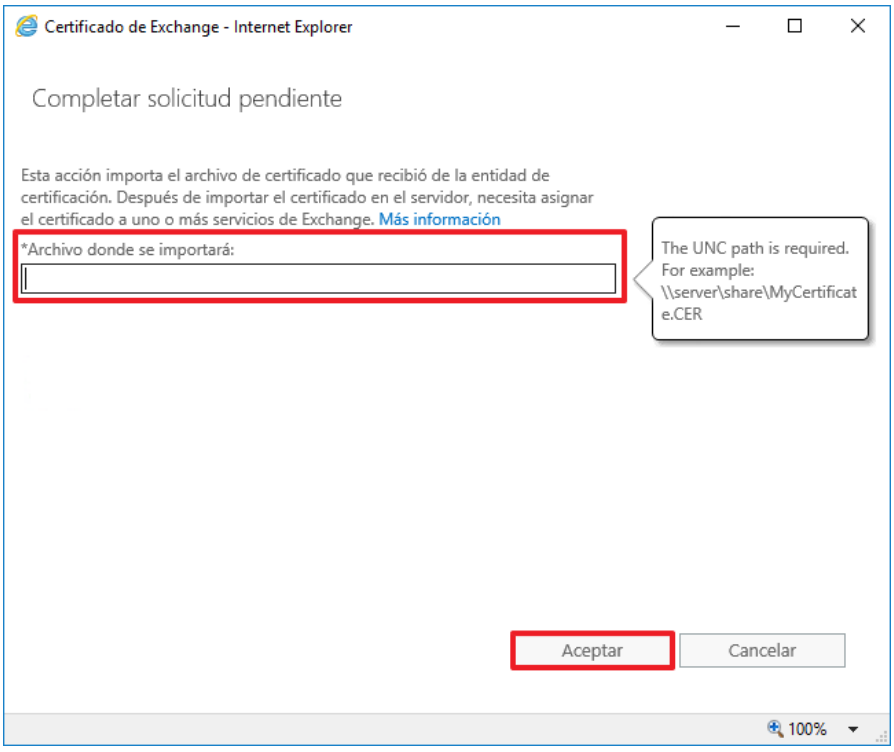
Sin embargo, el certificado autofirmado no es el más recomendable a la hora de implementar mecanismos de seguridad que requieran la confianza de clientes y usuarios ya que es relativamente sencillo suplantar la identidad de un certificado de estas características. Para evitar esto, se requiere la emisión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

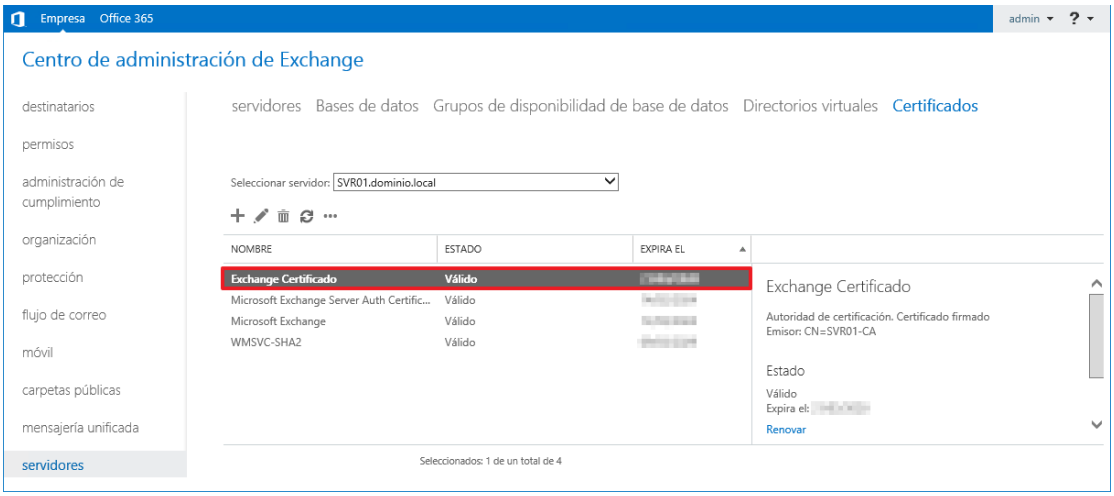
La implementación de certificados puede realizarse bien empleando certificados emitidos por una entidad certificadora que la organización haya implementado o bien por un certificado adquirido a una entidad certificadora de terceros como puede ser la FNMT (Fábrica Nacional de Moneda y Timbre).

A continuación, se muestra un ejemplo de cómo instalar un certificado emitido por una entidad certificadora autorizada, en este paso a paso se da por hecho que ya se ha solicitado un certificado a una entidad de certificación autorizada y se ha obtenido el certificado por lo que se explicara cómo instalarlo.

Paso	Descripción
97.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
98.	Pulse sobre "Internet Explorer" en la barra de tareas. 
99.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.

Paso	Descripción
100.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
101.	Seleccione en el menú lateral izquierdo la opción "servidores" y a continuación seleccione "Certificados".  **Nota:** En este ejemplo se da por hecho que se ha solicitado previamente un certificado emitido por una entidad certificadora autorizada para este servidor.

Paso	Descripción
102.	Seleccione el certificado el cual solicito previamente, y se encuentra en estado "Pedido pendiente". Pulse en el lateral derecho de la pantalla sobre "completo" para finalizar la instalación del certificado. 
103.	A continuación, seleccione el certificado .cer obtenido y pulse sobre "Aceptar". 

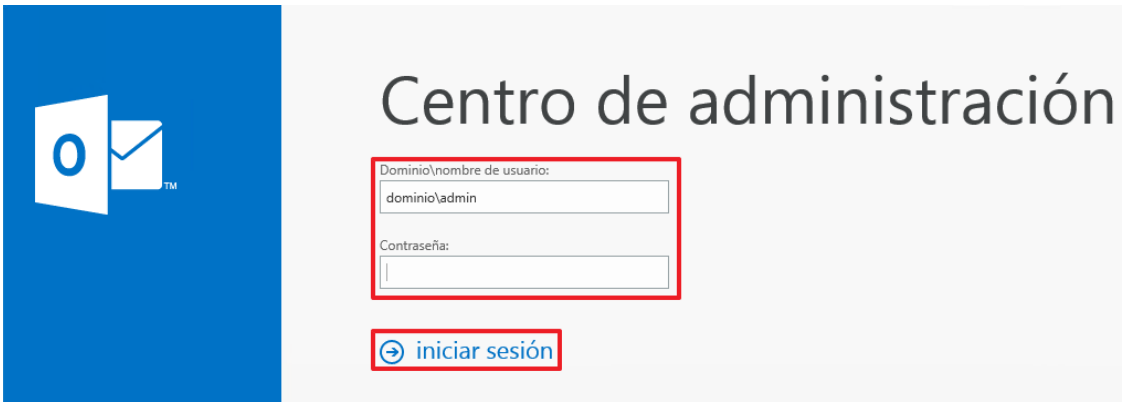
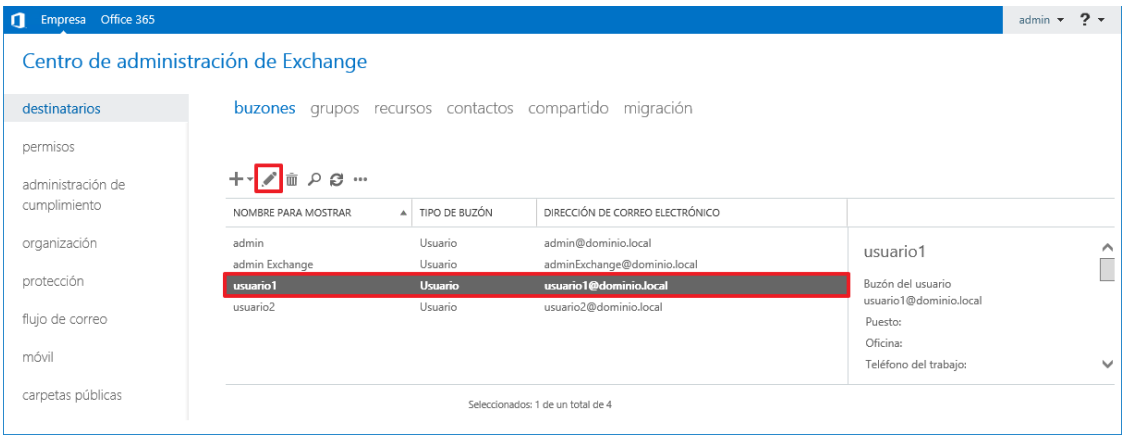
Paso	Descripción
104.	Compruebe que el estado del certificado instalado es válido y está asignado a los servicios que solicitó previamente. 

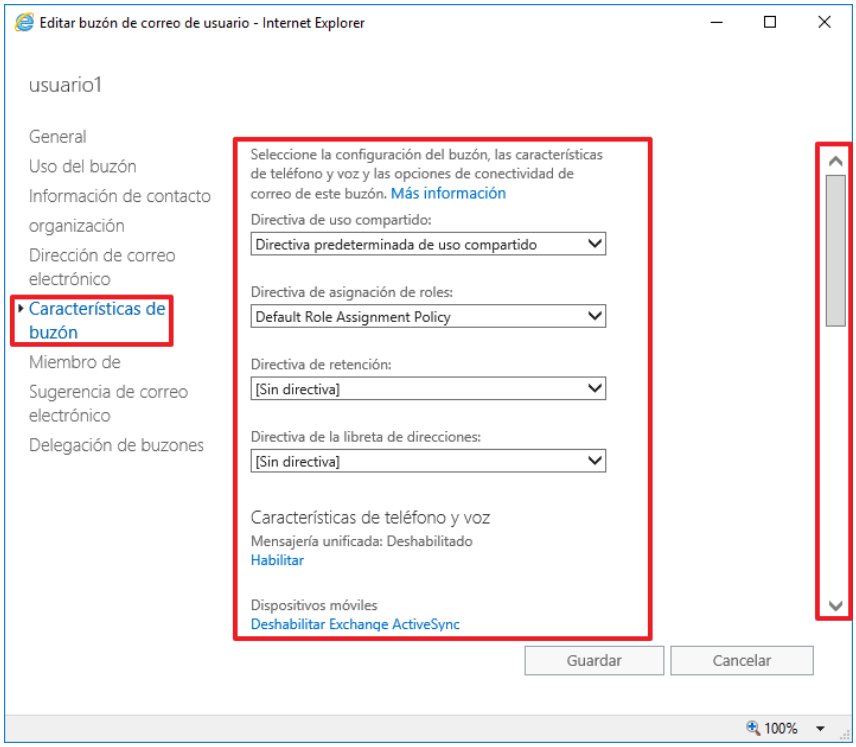
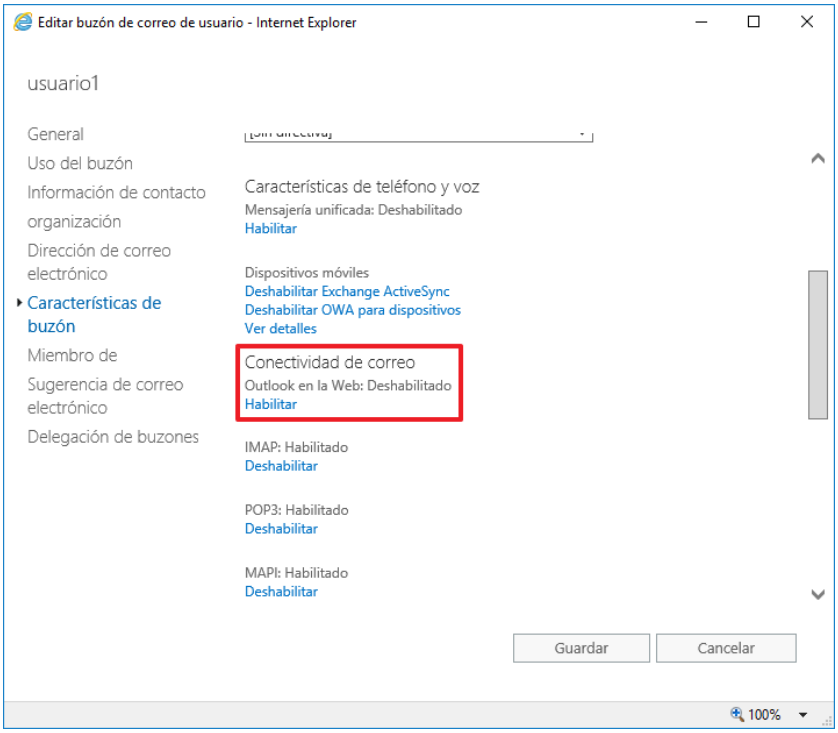
3.6. CONFIGURACIÓN DE SEGURIDAD

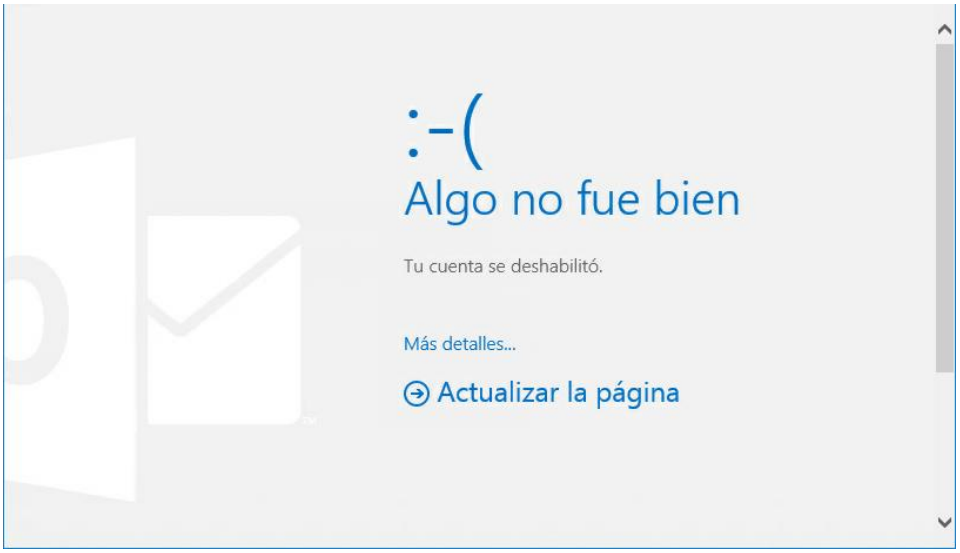
Microsoft Exchange Server 2016 instala POP3 e IMAP por defecto, pero los servicios se encuentran deshabilitados por lo que si es necesario su uso para su organización deberá habilitarlos manualmente.

En esta guía se va a usar el ejemplo de cómo deshabilitar una funcionalidad de Microsoft Exchange Server 2016 como principio de mínima funcionalidad y mínima exposición, deshabilitando la conectividad de correo Outlook Web App para aquellos buzones que no van a hacer uso de esta funcionalidad, limitando con ello, la exposición y aumentando la seguridad de la organización.

Paso	Descripción
105.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
106.	Pulse sobre "Internet Explorer" en la barra de tareas. 

Paso	Descripción
107.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.
108.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
109.	Seleccione el usuario o buzón en el que desea modificar alguna de las funcionalidades editándolo. Para ello seleccione el buzón que desea editar y pulse "Modificar". 

Paso	Descripción
110.	A continuación, Seleccione del menú lateral izquierdo la opción de "Características de buzón" y seleccione la configuración de buzón según las necesidades de su organización. 
111.	Para realizar este ejemplo se ha deshabilitado la conectividad de correo: Outlook Web App, en el "usuario1" creado en los pasos anteriores. 

Paso	Descripción
112.	Para comprobar el funcionamiento, al intentar acceder al buzón usando la funcionalidad de OWA, https://nombre_servidor/owa, devuelve un error indicando que la cuenta esta deshabilitada. 

3.7. TAREAS DE MANTENIMIENTO

El fabricante de Microsoft Exchange Server 2016 publica periódicamente una serie de actualizaciones acumulativas que corrigen nuevas vulnerabilidades detectadas, dichas actualizaciones deben ser instaladas para cumplir con el ENS.

Microsoft Exchange Server 2016 no se actualiza automáticamente por lo que para actualizar el producto deberá descargar manualmente las actualizaciones de la página del fabricante.

Para el cumplimiento del ENS es recomendable realizar todas las tareas de actualización previamente en un entorno de test controlado que refleje el entorno de producción de su organización.

Antes de proceder a realizar una actualización acumulativa de Microsoft Exchange Server 2016, es recomendable realizar un backup previo del estado de los controladores de Active Directory, del rol de Mailbox (backup completo de las bases de datos) y del Client Access (Backup del IIS), además se tendrá que tener en consideración posibles personalizaciones del código por ejemplo de la interfaz gráfica del Outlook Web App el cual deberá ser respaldado para no sufrir pérdidas durante la instalación de la actualización.

Nota: Si desea obtener más información sobre las actualizaciones acumulativas de Microsoft Exchange Server 2016 visite el sitio web: https://technet.microsoft.com/es-es/library/hh135098(v=exchg.150).aspx.

3.8. REGISTRO DE ACTIVIDAD

Con la aplicación del ENS para la categoría alta - DL sobre Exchange Server 2016 quedará registrado el uso del sistema para poder detectar y reaccionar a cualquier fallo accidental o deliberado, quedando registrado en el sistema quien realiza la actividad, cuando y sobre qué información con el fin de detectar anomalías o intentos frustrados de acceso a información no autorizada.

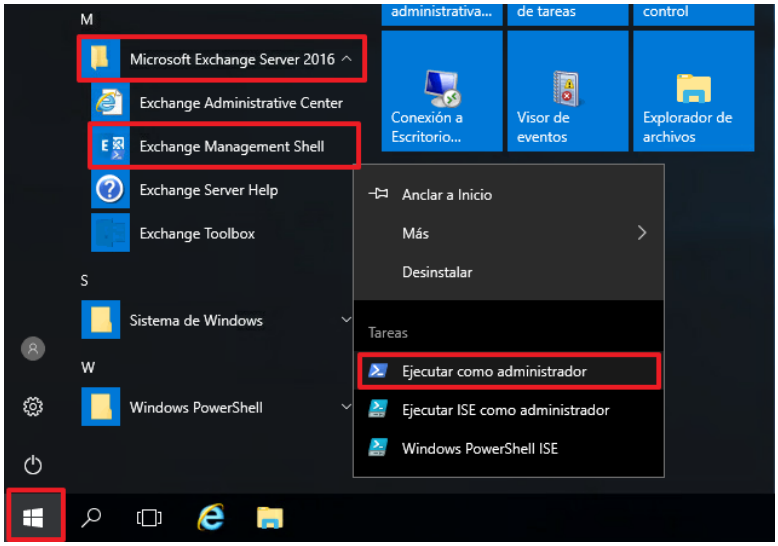
Es recomendable que la ubicación de los registros sea diferente a la del sistema además de tener limitado el acceso únicamente a los usuarios autorizados.

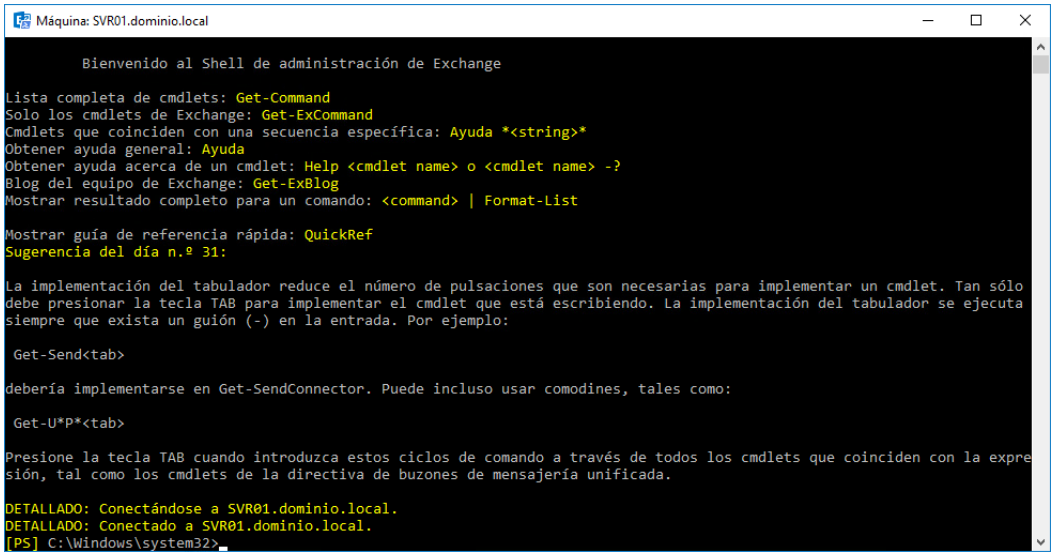
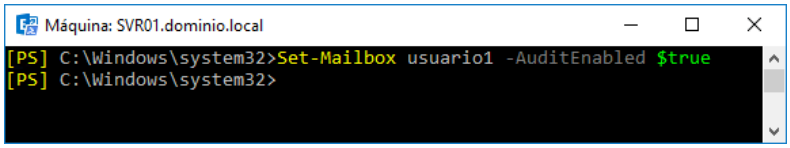
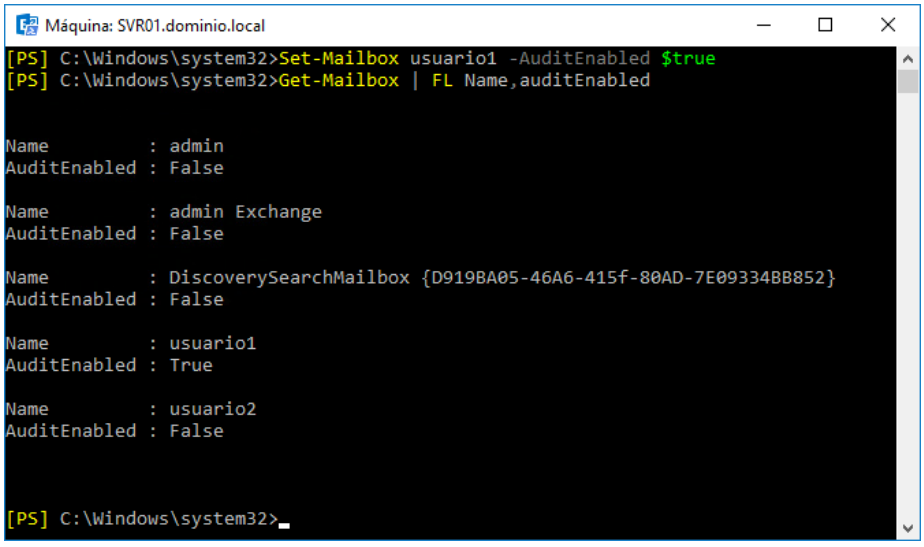
Mediante el registro de auditoría de buzón, se puede registrar el acceso y controlar los inicios de sesión a los buzones de correo por parte de sus propietarios, delegados (incluidos los administradores con permisos de acceso total al buzón) y administradores.

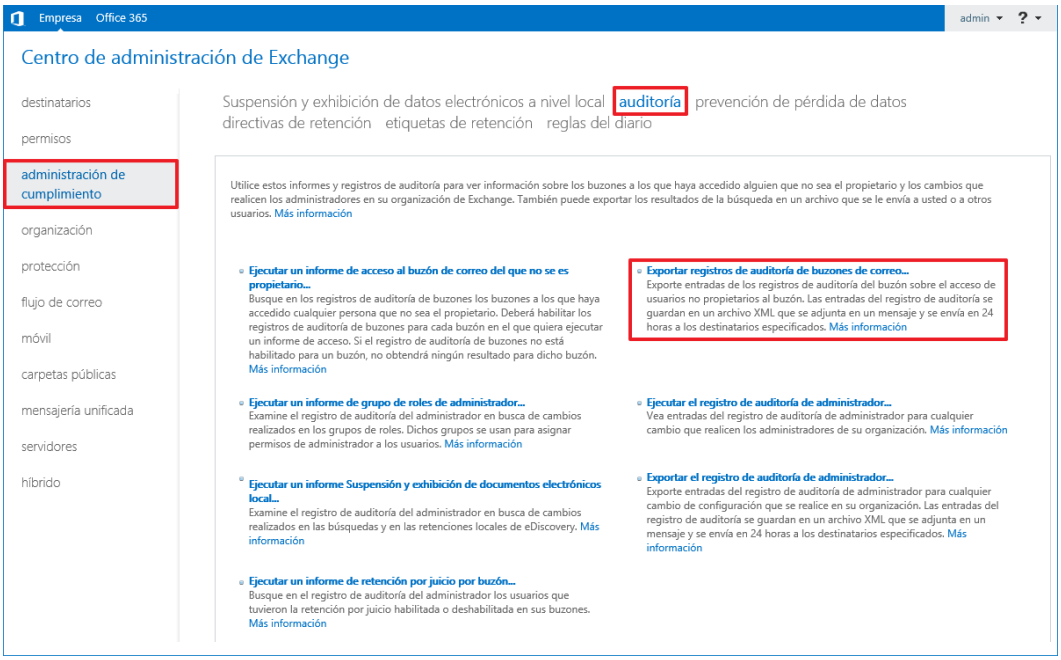
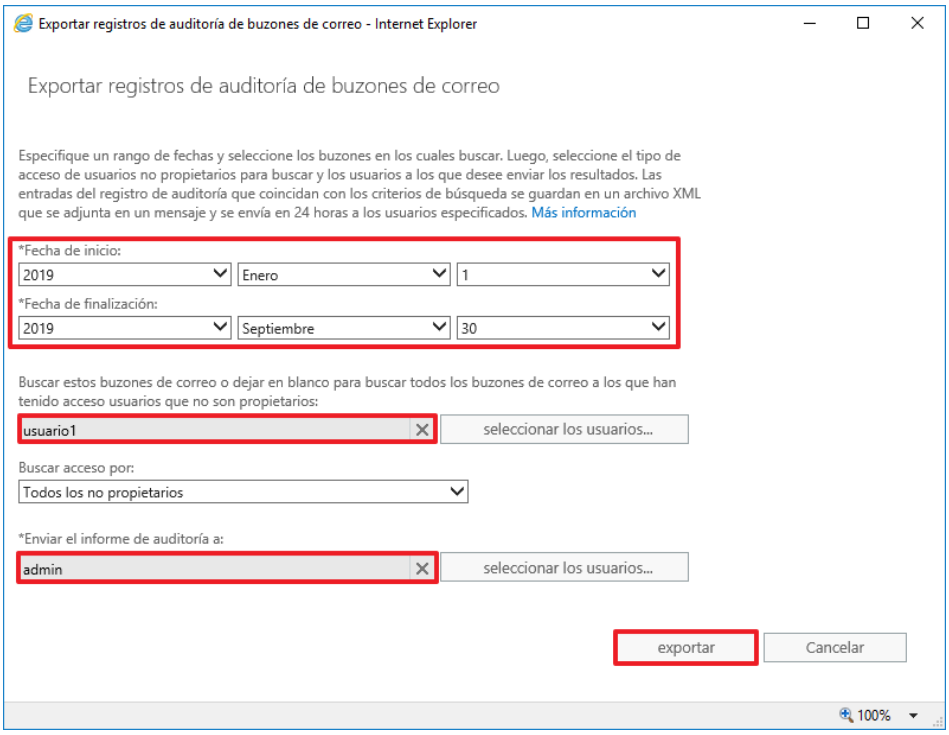
La auditoría de las acciones del propietario del buzón puede generar una gran cantidad de entradas en el registro de auditoría, por lo que se encuentra deshabilitada de forma predeterminada. Se recomienda activar solo la auditoría de algunas acciones específicas necesaria para cumplir con los requisitos comerciales o de seguridad.

Cuando un buzón de correo tiene habilitada la auditoría, Microsoft Exchange Server 2016 guarda la información de accesos al buzón y los elementos del buzón en el registro de auditoría de buzones de correo, siempre que un usuario que no sea el propietario obtenga acceso al buzón de correo.

Cada entrada de registro incluye información acerca de quién tuvo acceso al buzón y en qué momento, así como las acciones realizadas por el usuario que es no propietario y si la acción se realizó correctamente.

Paso	Descripción
113.	Inicie sesión en el servidor miembro donde está instalado Microsoft Exchange Server 2016 con un usuario con permisos de administrador.
114.	Pulse sobre el menú inicio despliegue la carpeta "Microsoft Exchange Server 2016" y pulsando con botón derecho en "Exchange Management Shell" seleccione "Ejecutar como administrador".  **Nota:** El sistema le solicitará elevación de privilegios.

Paso	Descripción
115.	A continuación, se mostrará la siguiente ventana. 
116.	Una vez conectado al Shell, ejecute la siguiente sintaxis. – Set-Mailbox <identity> -AuditEnabled $true  **Nota:** En este ejemplo se habilita la auditoría para el buzón de "usuario1".
117.	Para conocer los buzones donde se encuentra habilitada la auditoria, se puede ejecutar el siguiente cmdlet. – Get-Mailbox | FL Name,auditEnabled 

Paso	Descripción
118.	Es posible exportar los registros de auditoría de buzones desde la consola Web de administración de Exchange desde el menú "administración de cumplimiento" seleccionando la opción "Auditoría", tal y como se ha podido observar en el punto anterior.  **Nota:** Exchange puede tardar hasta 24 horas en generar el informe y enviarlo al destinatario seleccionado
119.	Deberá indicar el intervalo de fechas, los buzones en dónde realizar la búsqueda y el buzón de destino del informe. 

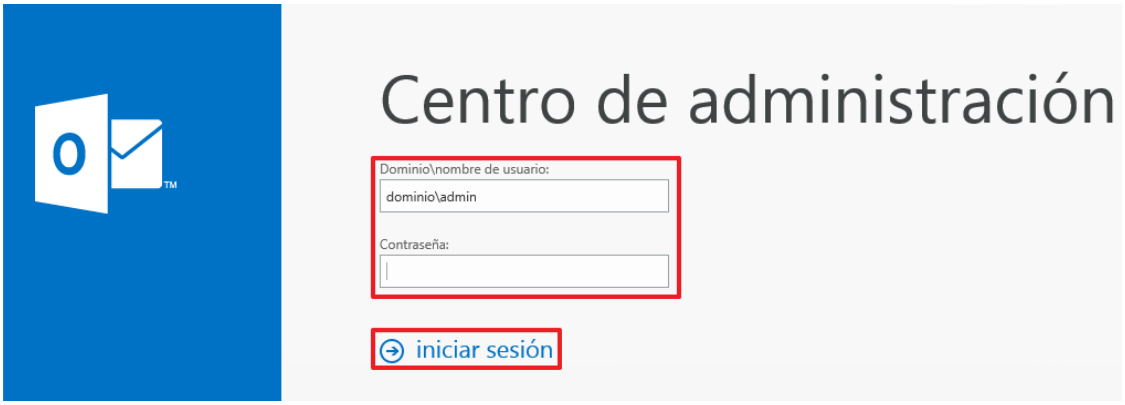
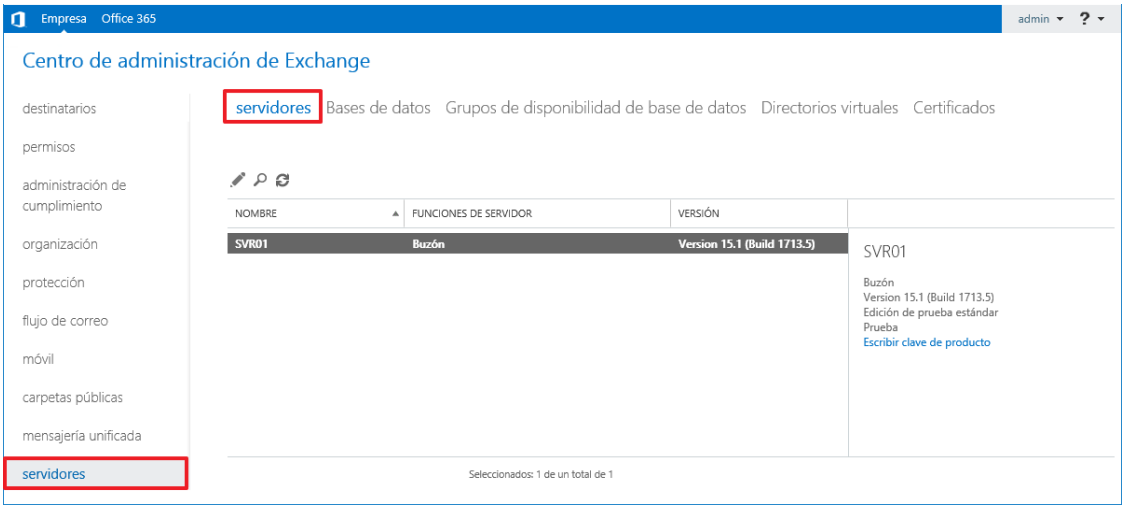
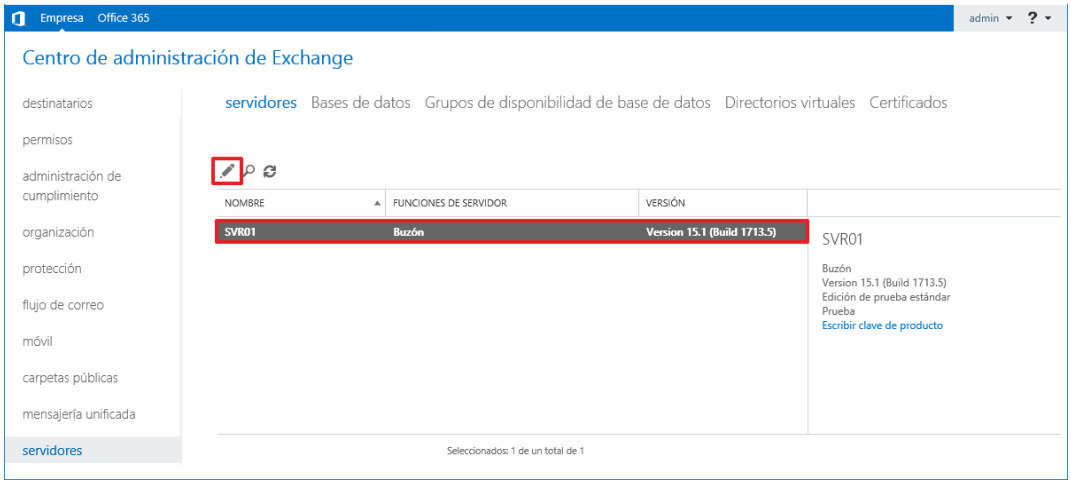
Paso	Descripción
120.	El resultado lo recibirá en su buzón el usuario especificado en la ventana de exportación de registros de auditoría. **Nota:** Debe tener en consideración que, si visualiza el informe desde Outlook Web App, de forma predeterminada se bloquea el acceso a los ficheros ".xml". Si quiere permitir que en Outlook Web App sean accesibles los ficheros ".xml", consulte la información que proporciona Microsoft en el siguiente enlace: https://technet.microsoft.com/es-es/library/jj150552(v=exchg.150).aspx.

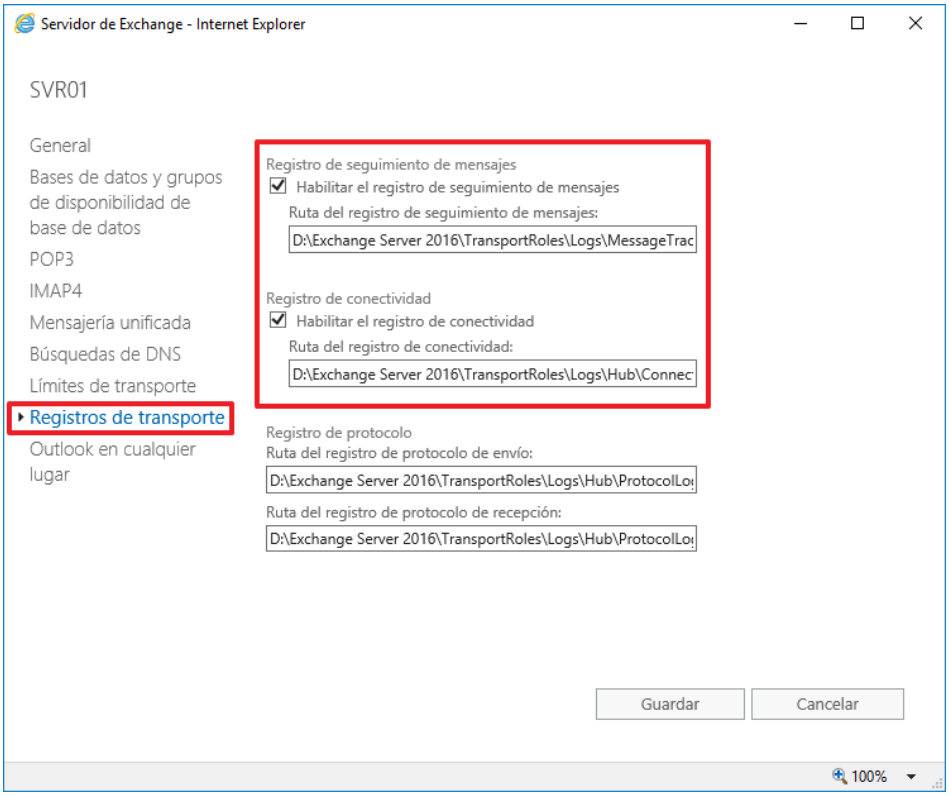
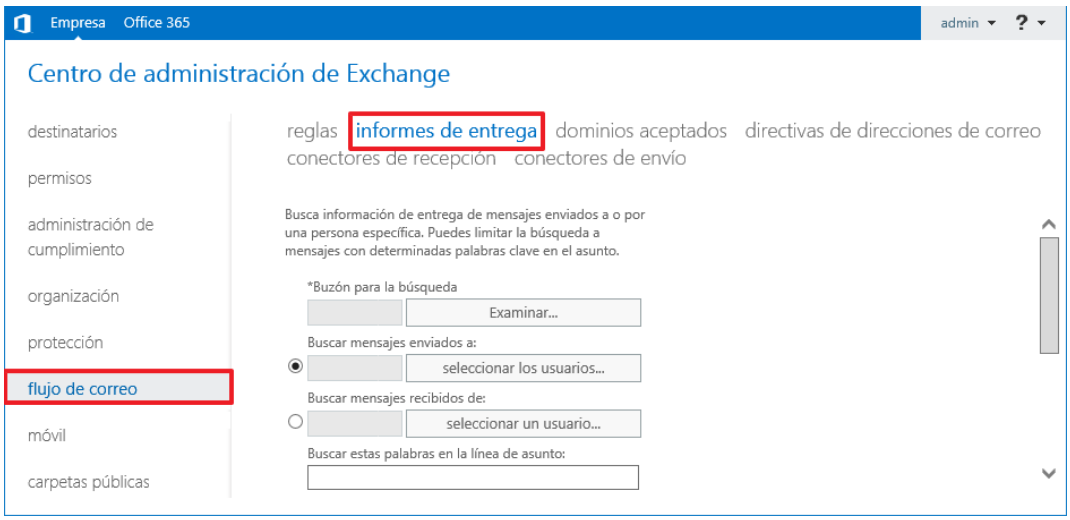
3.9. REGISTRO DE SEGUIMIENTO DE MENSAJES

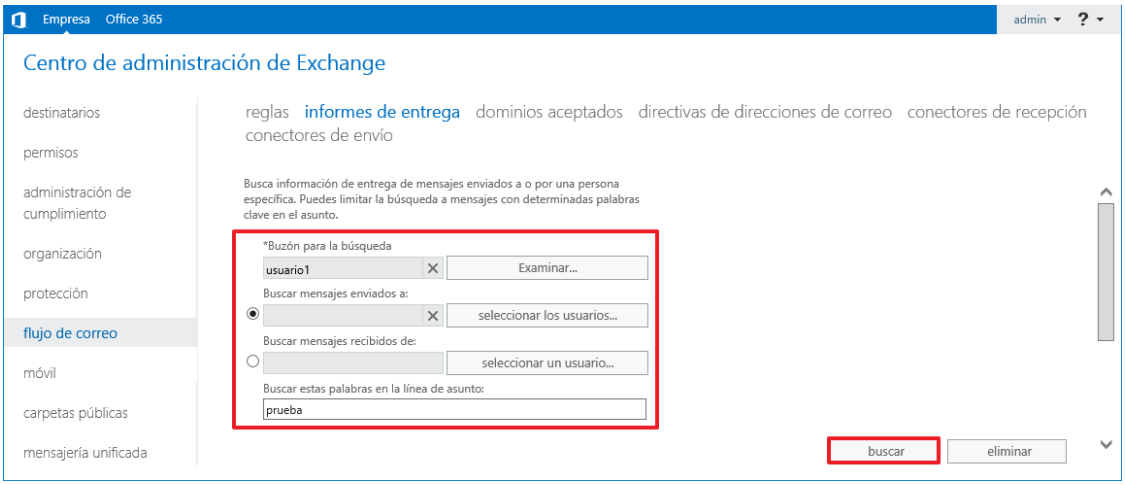
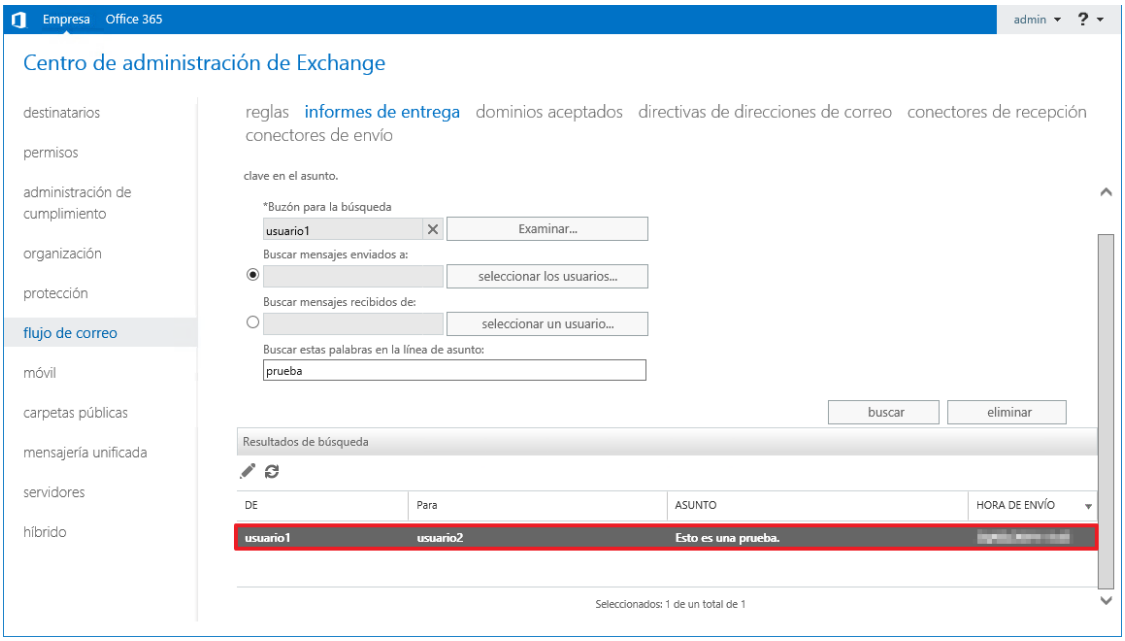
De forma predeterminada, Microsoft Exchange Server 2016 implementa mecanismos de registro para el seguimiento de mensajes y la conectividad de diferentes protocolos. Estos incluyen el envío y recepción de correos, así como la capacidad para analizar el estado de los mismos.

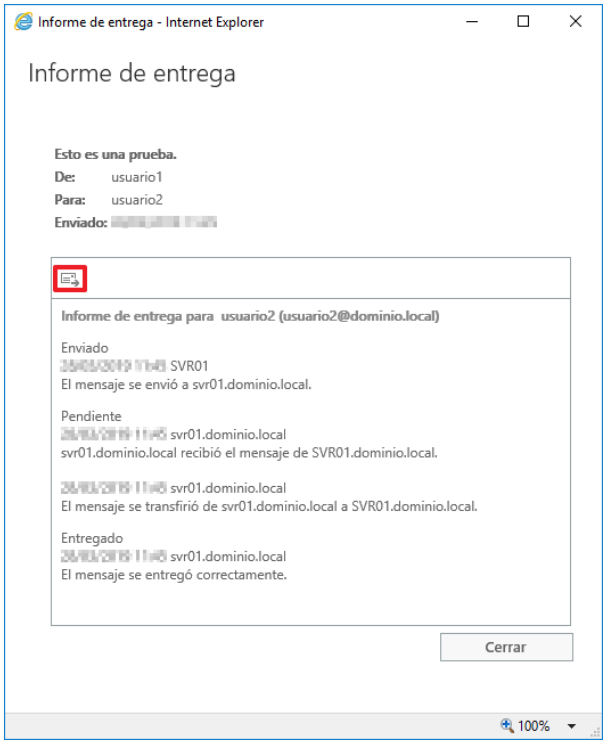
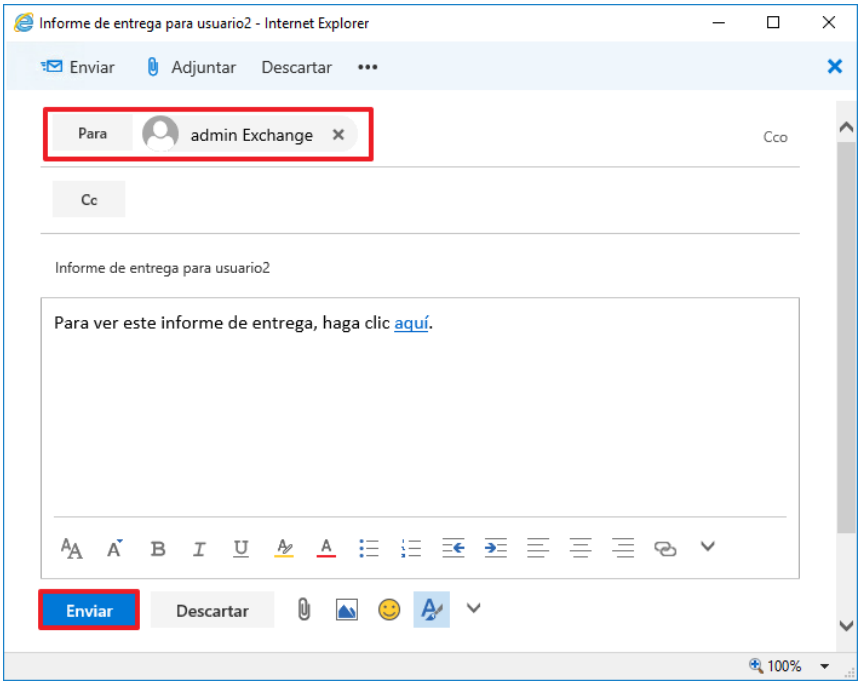
El seguimiento de mensajes se encuentra habilitado, así como los registros de protocolos de comunicaciones, pero podría necesitar modificarlos o bien si han sido desactivados en un momento determinado, poder habilitarlos nuevamente.

Paso	Descripción
121.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
122.	Pulse sobre "Internet Explorer" en la barra de tareas. 
123.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.

Paso	Descripción
124.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
125.	Dentro de la consola de administración de Exchange, seleccione el menú "servidores". A continuación, seleccione "servidores". 
126.	Seleccione el servidor con el rol "Buzón" y a continuación el botón de "Modificar" para dicho servidor. 

Paso	Descripción
127.	En la sección "Registros de transporte" puede modificar la configuración de almacenamiento de cada uno de los registros, así como habilitar y deshabilitar el "Registro de seguimiento de mensajes" y el "Registro de conectividad", tal y como se muestra a continuación. 
128.	Una vez modificadas las propiedades de acuerdo a las necesidades de su organización, pulse el botón "Guardar".
129.	El registro de seguimiento de seguimiento de mensajes lo puede ejecutar desde la propia consola Web de administración de Exchange Server 2016. Para ello, pulse sobre "flujo de correo" y posteriormente en "informes de entrega". 

Paso	Descripción
130.	Puede seleccionar el buzón en el que se desea buscar un mensaje, así como el remitente y/o el destinatario. Con la finalidad de reducir el número de resultados, se pueden escribir palabras clave en la línea de asunto (recuerde que esta funcionalidad sólo permite buscar por el asunto del mensaje y no su contenido).  **Nota:** En este ejemplo se ha utilizado el buzón "Usuario1" y la palabra clave "prueba".
131.	Los resultados se visualizarán en la zona inferior de la pantalla. Pulsando dos veces sobre cada uno de los resultados, se puede obtener un informe de seguimiento del mensaje. 

Paso	Descripción
132.	Así mismo, es posible que necesite enviar el informe de seguimiento al usuario afectado. Para ello pulse sobre el botón de envío y se generará un mensaje con un enlace para que el propio usuario lo pueda visualizar. 
133.	Especifique el destinatario y pulse sobre el botón "Enviar" para enviar el informe de entrega. 
134.	Una vez completadas las búsquedas de seguimiento de mensajes, pulse sobre el botón "Cerrar" y, a continuación, puede cerrar la sesión de la consola Web de administración de Exchange Server 2016.

3.10. REGISTRO DE LA GESTIÓN DE INCIDENTES

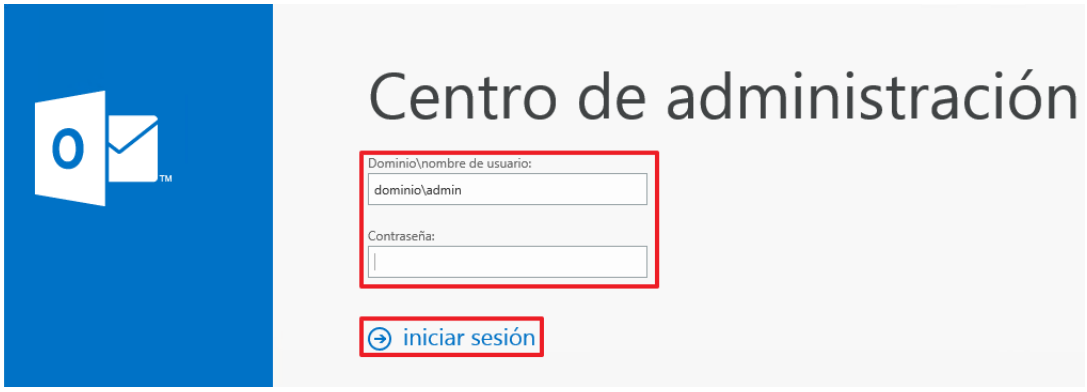
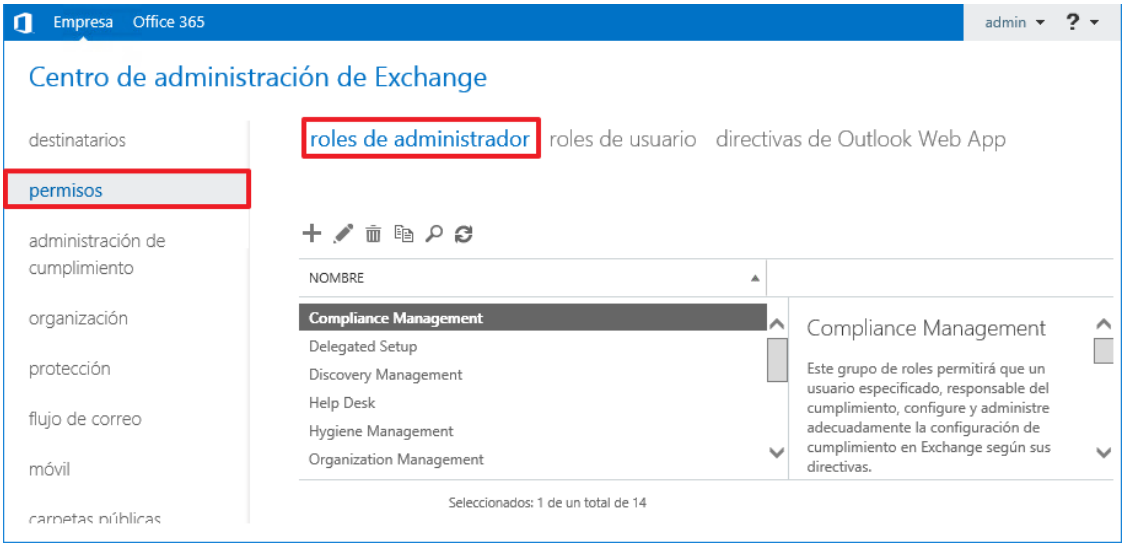
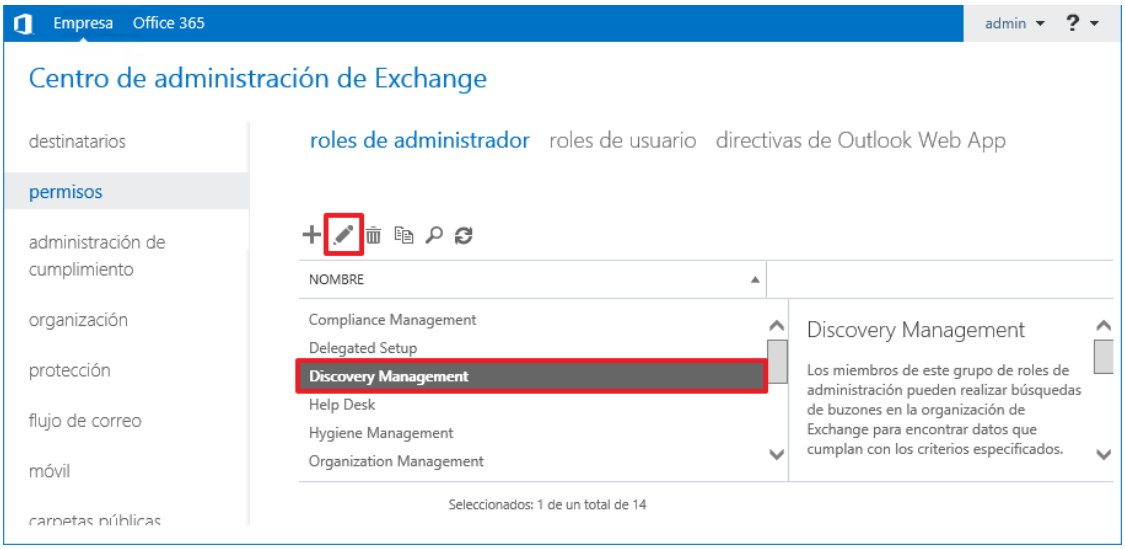
Microsoft Exchange Server 2016 contiene la funcionalidad de retención por juicio, también conocida como retención legal, la cual permite preservar la información almacenada electrónicamente. Cuando se habilita la retención por juicio a un buzón de un usuario, este usuario podrá eliminar elementos del buzón de correo, pero dichos elementos eliminados se retendrán en los servidores. La retención por juicio mantiene los mensajes de correo electrónico, los elementos de calendario, las tareas y otros elementos de buzón de correo, además la retención por juicio protege la versión original de cada elemento del buzón contra una modificación del usuario, por ejemplo, si un usuario cambia las propiedades de los elementos de un buzón y está habilitada la función de retención por juicio, se conserva una copia del elemento antes de que se produzca el cambio.

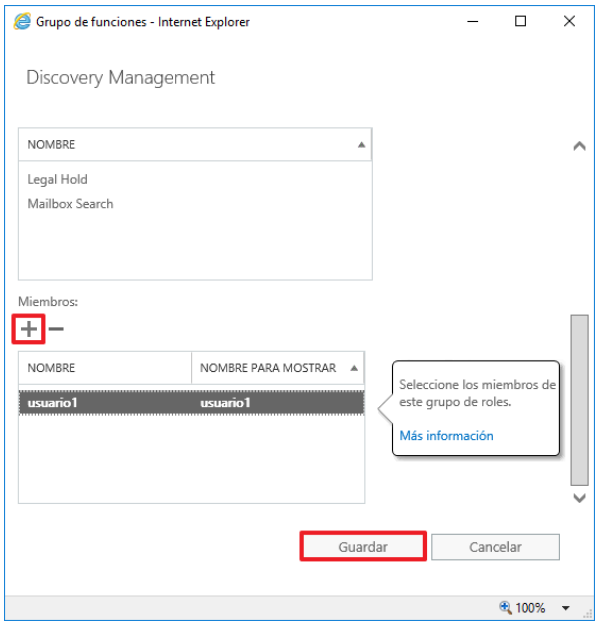
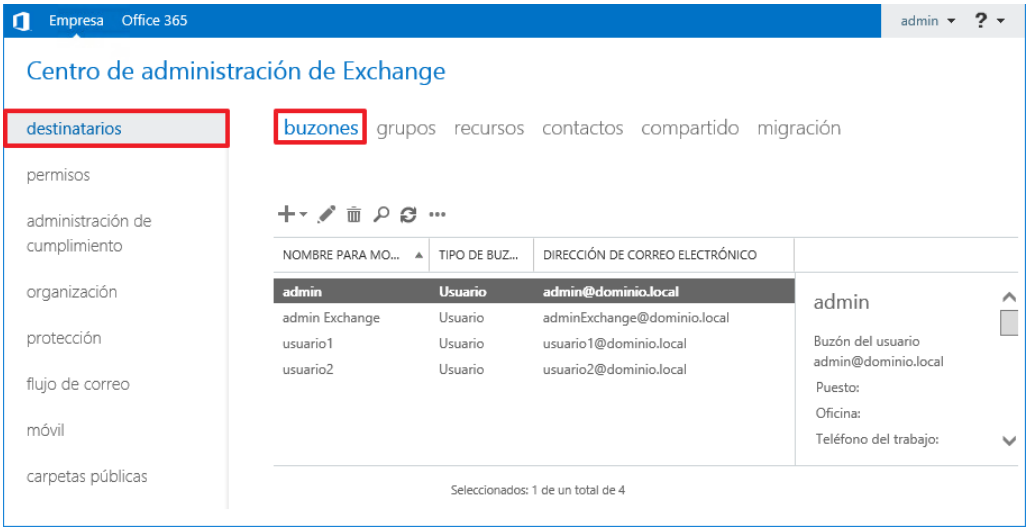
Los usuarios autorizados que han sido agregados al rol de gestión "Discovery Management" o al rol de gestión "Legal Hold", pueden poner buzones de usuarios en el modo de retención legal.

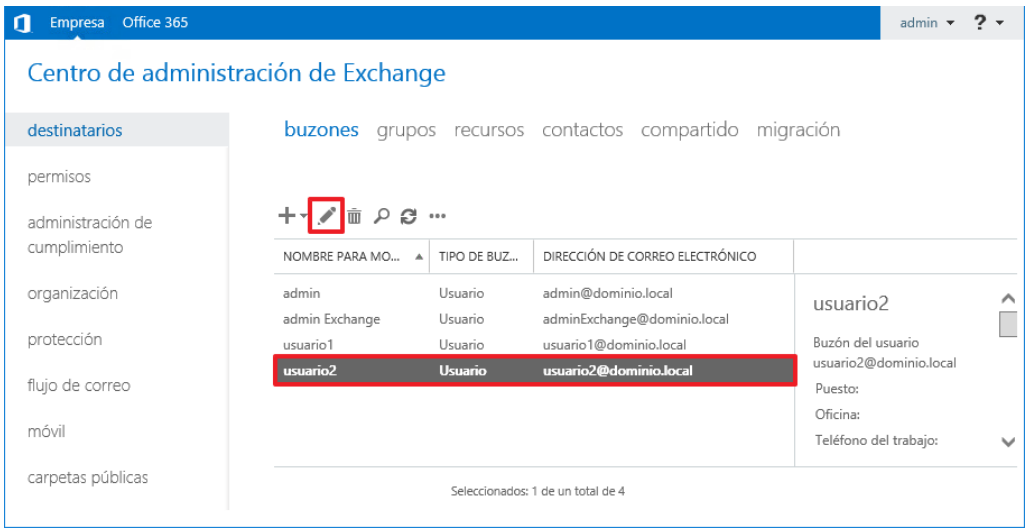
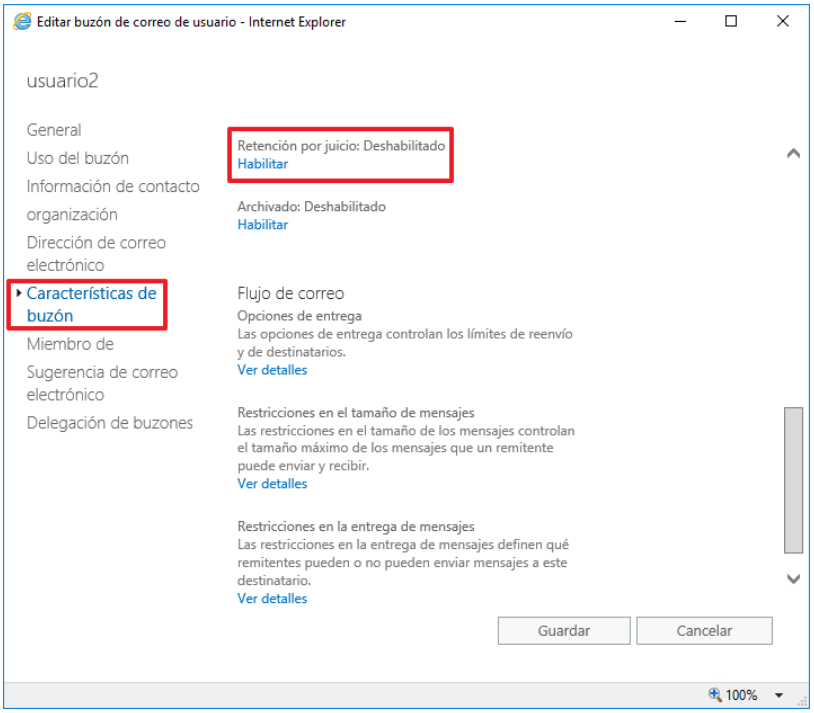
Para habilitar la funcionalidad de retención legal y realizar un análisis de buzones con la opción de retención legal habilitada, el usuario al que se quiera permitir la auditoría, deberá pertenecer al menos al grupo de roles predeterminado "Discovery Management".

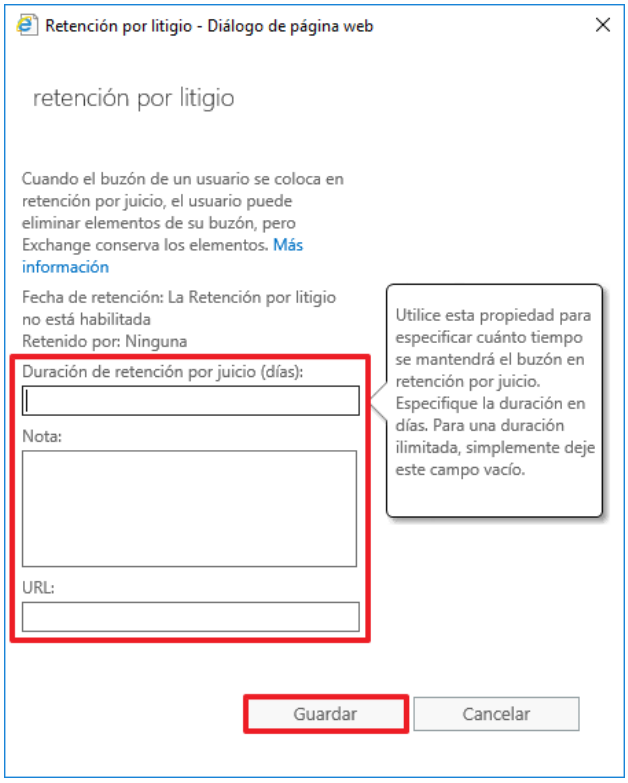
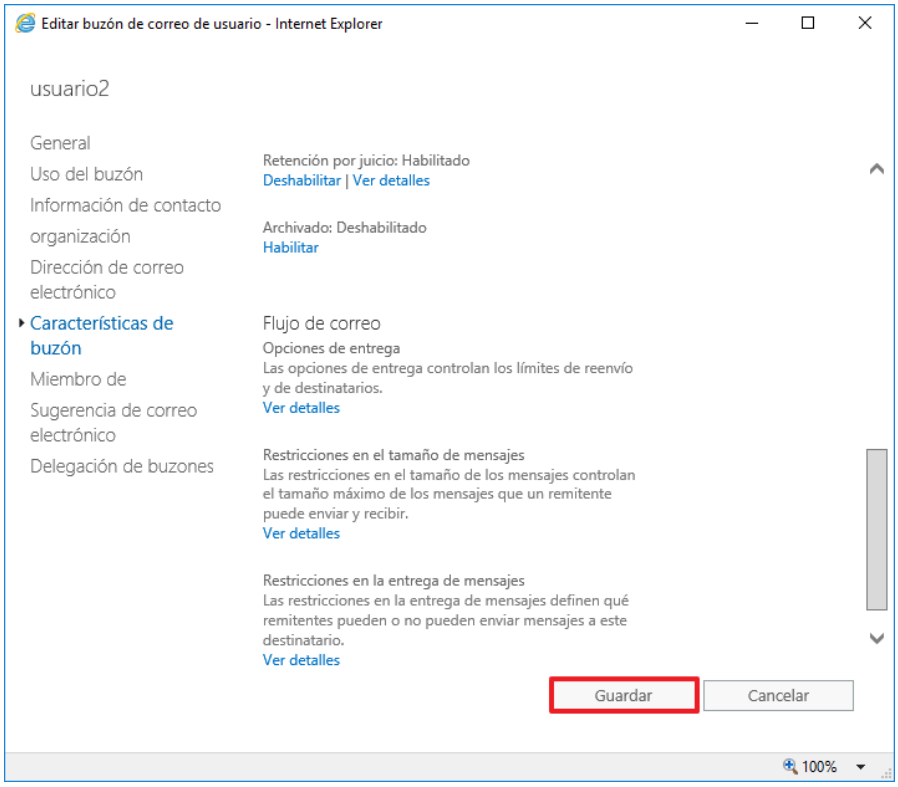
A continuación, se muestra cómo añadir un usuario al grupo de roles predeterminado "Discovery Management" y cómo habilitar la retención legal en un buzón de usuario.

Paso	Descripción
135.	Inicie sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
136.	Pulse sobre "Internet Explorer" en la barra de tareas. 
137.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.

Paso	Descripción
138.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
139.	Seleccione "permisos" y a continuación sitúese en "roles de administrador". 
140.	A continuación, seleccione el grupo de roles "Discovery Management" y pulse "Editar". 

Paso	Descripción
141.	En la sección "Miembros", pulse sobre el botón "+" para agregar las cuentas de los usuarios a los cuales se les quiere otorgar este grupo de roles, para finalizar pulse sobre "Guardar".  **Nota:** En este ejemplo se agrega la cuenta DOMINIO\usuario1 creada previamente, debe adaptar estos pasos a su organización. Además, cabe señalar que los administradores de la organización Exchange, de forma predeterminada no disponen de los permisos para realizar búsquedas en los buzones de tipo suspensión y exhibición de datos electrónicos, aunque sí disponen del permiso para establecer un buzón en modo de retención legal.
142.	A continuación, para habilitar la retención por juicio en un buzón de usuario, diríjase a la sección **"destinatarios → buzones"**. 

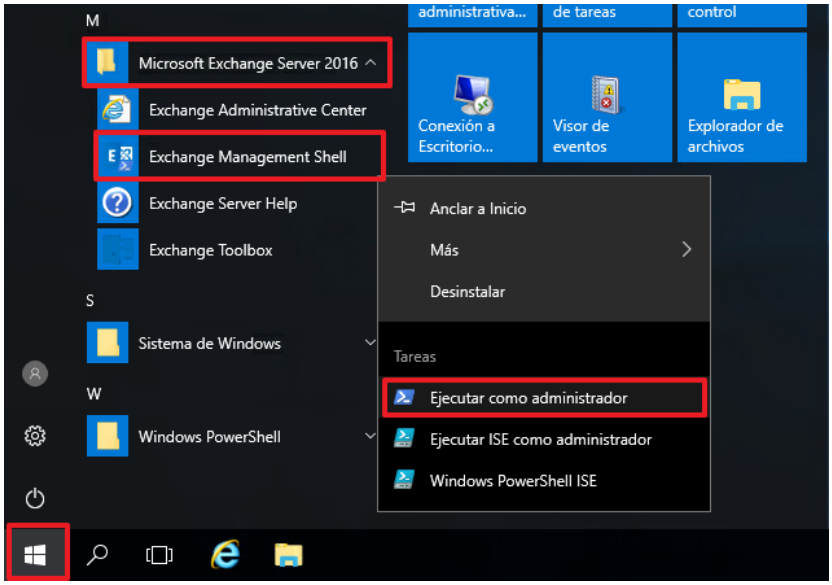
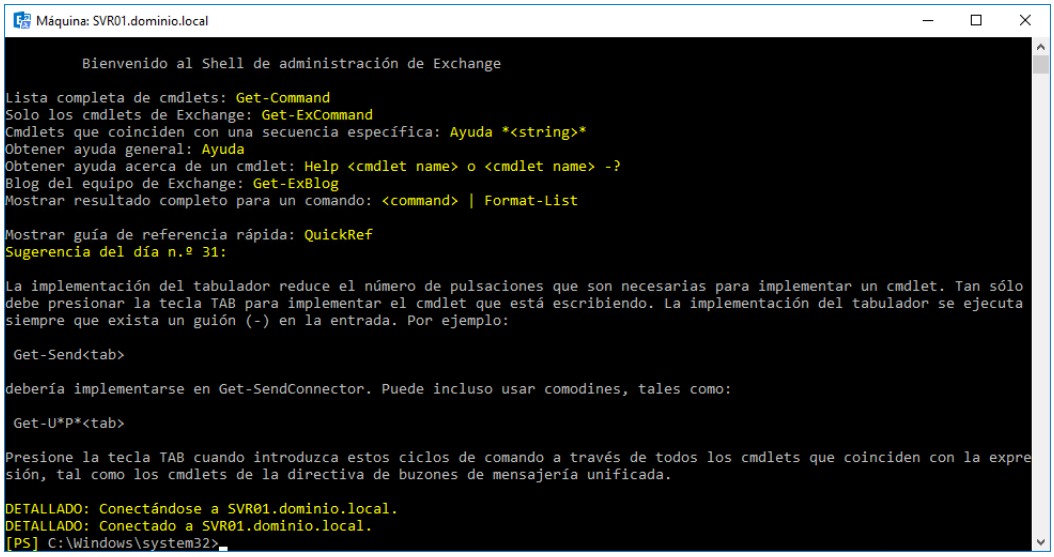
Paso	Descripción
143.	Seleccione el buzón de usuario en el cual desea habilitar la retención por juicio y pulse sobre "Modificar".  **Nota:** En este ejemplo se activará la retención por juicio al "usuario2".
144.	En la sección "Características de buzón", pulse sobre el botón "Habilitar" en "Retención por juicio" para activar la retención por juicio sobre el buzón de usuario previamente seleccionado. 

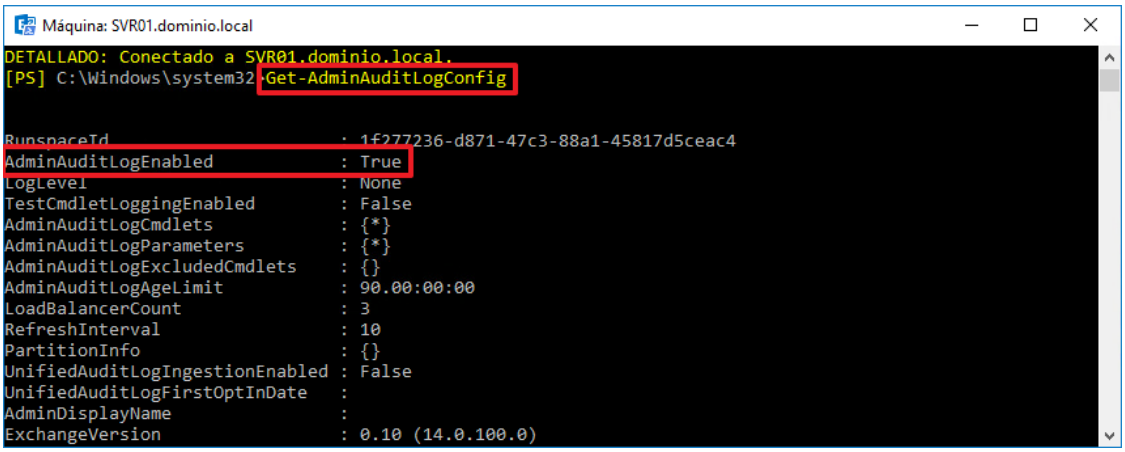
Paso	Descripción
145.	A continuación, complete la siguiente ventana adecuándola a las necesidades de su organización y pulse sobre "Guardar". 
146.	Una vez finalizada la configuración pulse sobre "Guardar" para cerrar la ventana. 

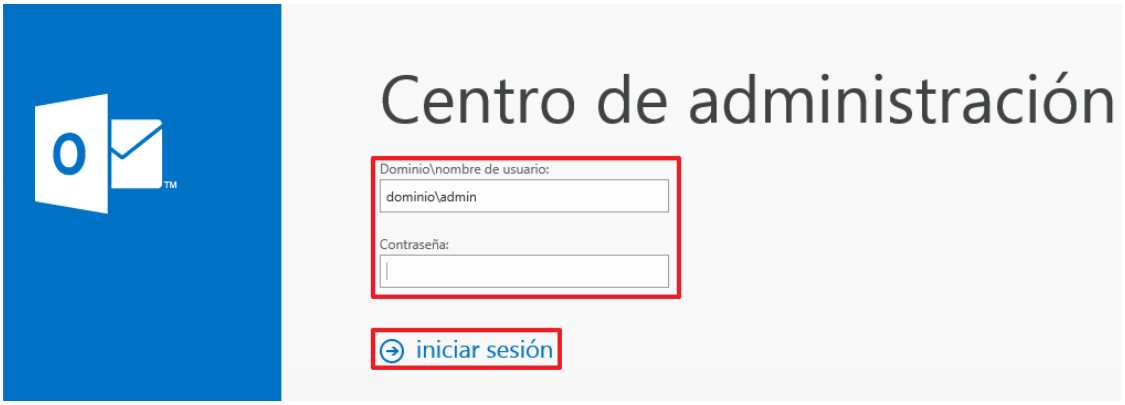
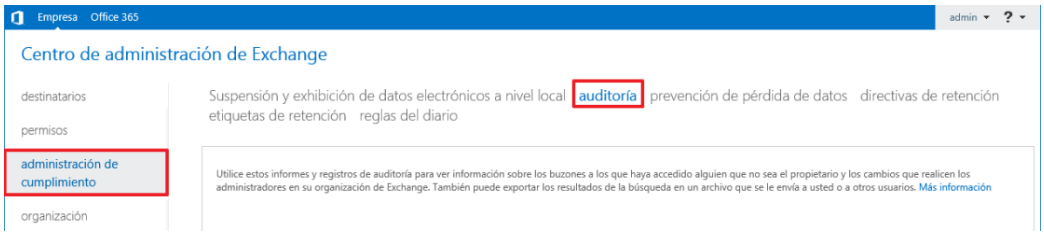
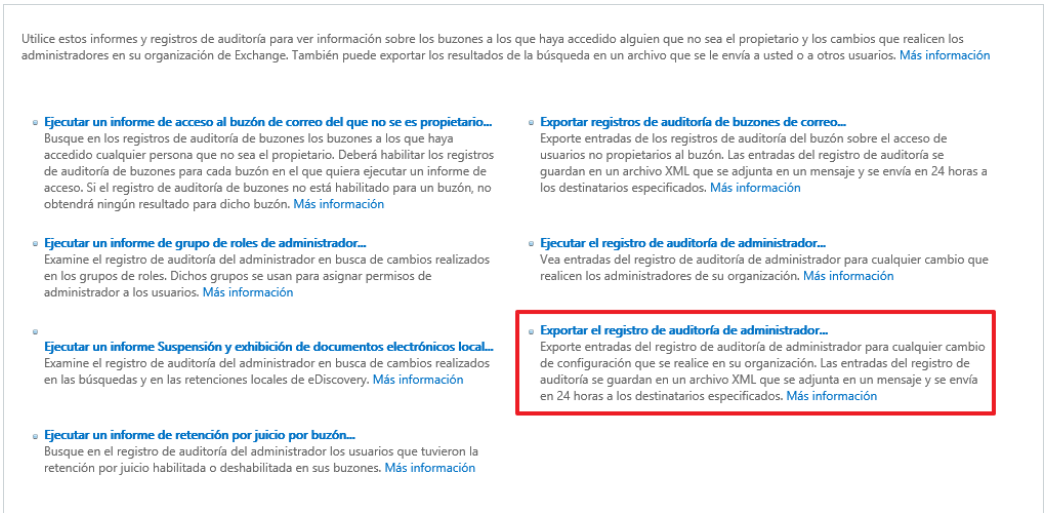
Paso	Descripción
147.	Pulse "Aceptar" en la advertencia. 
148.	Una vez habilitada la retención legal en los buzones correspondientes, es posible obtener un informe sobre los elementos que han sido modificados o eliminados desde el menú **"Administración del cumplimiento → Auditoría"** en la consola Web de administración de Exchange Server 2016. 

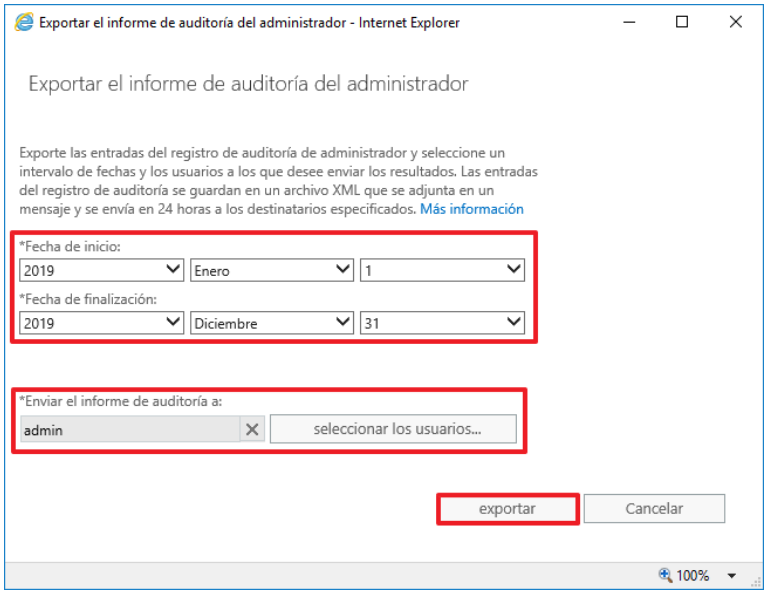
3.11. PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD

A través del registro de auditoria del administrador se pueden ver las operaciones de administración ejecutadas por usuarios o administradores en Exchange Server 2016. De forma predeterminada se encuentra habilitado, no obstante, se muestra a continuación cómo ver el estado, habilitarlo en el caso de que no lo estuviera y acceder a la información almacenada en dicho registro.

Paso	Descripción
149.	Inicie sesión en el servidor miembro donde está instalado Microsoft Exchange Server 2016 con un usuario con permisos de administrador.
150.	Pulse sobre el menú inicio despliegue la carpeta "Microsoft Exchange Server 2016" y pulsando con botón derecho en "Exchange Management Shell" seleccione "Ejecutar como administrador".  **Nota:** El sistema le solicitará elevación de privilegios.
151.	A continuación, se mostrará la siguiente ventana. 

Paso	Descripción
152.	A continuación, ejecute la siguiente sintaxis. – "Get-AdminAuditLogConfig" Con ello se comprobará si el registro de auditoria del administrador está habilitado.  **Nota:** En el caso de que el registro no se encontrase habilitado, podrá habilitarse ejecutando la siguiente sintaxis. - "Set-AdminAuditLogConfig –AdminAuditLogEnabled $True"
153.	La obtención de resultados correspondiente se puede realizar a través de la consola Web de Administración de Exchange 2016.
154.	La obtención de resultados correspondiente se puede realizar a través de la consola Web de Administración de Exchange 2016. El acceso a dicha herramienta se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
155.	Pulse sobre "Internet Explorer" en la barra de tareas. 
156.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.

Paso	Descripción
157.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".
158.	Una vez dentro de la consola Web de administración, seleccione el menú "administración de cumplimiento" y a continuación "auditoría". 
159.	En el menú de auditoría, se podrá realizar la exportación personalizada de los registros de auditoría del administrador. Para ello pulse sobre la opción "Exportar el registro de auditoría del administrador…". 

Paso	Descripción
160.	A continuación, deberá indicar las fechas de inicio y finalización del registro que se desea exportar y a que buzón se va a enviar el resultado. Una vez introducidos los datos pulse sobre el botón "Exportar".  **Nota:** Exchange puede tardar hasta 24 horas en generar el informe y enviarlo al destinatario seleccionado.
161.	Una vez transcurrido el tiempo necesario, el usuario al que se le ha enviado el informe de auditoría, recibirá una notificación con el resultado en formato xml. **Nota:** Debe tener en consideración que, si visualiza el informe desde Outlook Web App, de forma predeterminada se bloquea el acceso a los ficheros ".xml". Si quiere permitir que en Outlook Web App sean accesibles los ficheros ".xml", consulte la información que proporciona Microsoft en la siguiente URL: https://technet.microsoft.com/es-es/library/jj150552(v=exchg.150).aspx

3.12. PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD

Uno de los cambios más significativos desde Exchange 2013, es que RPC ya no es un protocolo de acceso directo compatible. Esto significa que la conectividad de Outlook en su totalidad debe realizarse a través del servidor de acceso de cliente mediante RPC sobre HTTP (también conocido como Outlook Anywhere).

El beneficio de este cambio es que no hay necesidad de tener el servicio de acceso de clientes de RPC en el servidor acceso de clientes. Esto ocasiona la reducción de dos espacios de nombres que habitualmente se necesitarían para una solución de resistencia ante fallos a nivel de sitios. Asimismo, ya no hay requerimientos para suministrar afinidad para el servicio de acceso de clientes de RPC.

Junto a esto, Exchange Server 2016 incorpora un protocolo de comunicación con los clientes Outlook denominado MAPI sobre HTTP (no confundir con RPC sobre HTTP o Outlook Anywhere).

MAPI sobre HTTP supone un avance importante en la simplificación de las comunicaciones de los clientes Outlook y el soporte de nuevos mecanismos de autenticación modernos como federación de identidades, autenticación de doble factor u otros.

MAPI sobre HTTP traslada la capa de transporte al modelo HTTP para mejorar la confiabilidad y la estabilidad de las conexiones de Outlook y Exchange. Esto permite un mayor nivel de visibilidad de los errores de transporte y una capacidad de recuperación mayor. Entre la funcionalidad adicional se incluye compatibilidad para una función de pausa y reanudación explícitas. Esto permite a los clientes compatibles cambiar de red o reactivarse después de la hibernación, manteniendo el mismo contexto de servidor.

Microsoft Exchange Server 2016 incorpora estas características por defecto desde su instalación, por lo que, si no se desea degradar la seguridad es recomendable no deshabilitar el uso de estos protocolos.

3.13. MEDIOS ALTERNATIVOS

En la categoría alta - DL del marco operacional del ENS se debe garantizar la existencia y disponibilidad de medios alternativos en caso de fallo de los medios habituales por lo que Exchange Server 2016 utiliza, tanto para la alta disponibilidad como para la resistencia de sitio, un concepto conocido como implementación incremental. Para implementar dicha funcionalidad se debe disponer de dos o más servidores de buzones de correo de Exchange 2016 como servidores independientes, y luego, configurarlos de manera incremental junto con las bases de datos de buzones de correo para que haya una alta disponibilidad y resistencia de sitios según sea necesario.

En Microsoft Exchange Server 2016, la alta disponibilidad de transporte es responsable de mantener copias redundantes de los mensajes antes y después de la entrega correcta de estos.

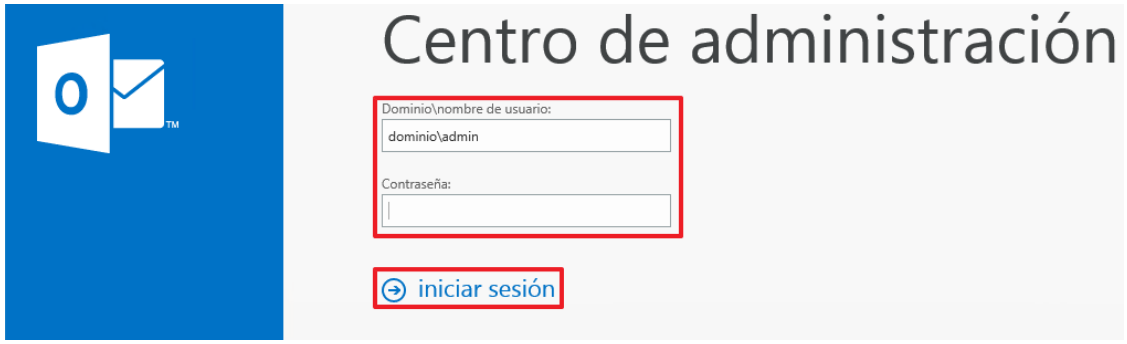
Exchange 2016 usa DAG y copias de bases de datos de buzones de correo, junto con otras funciones, para suministrar protección de datos nativa de Exchange, alta disponibilidad y resistencia de sitios.

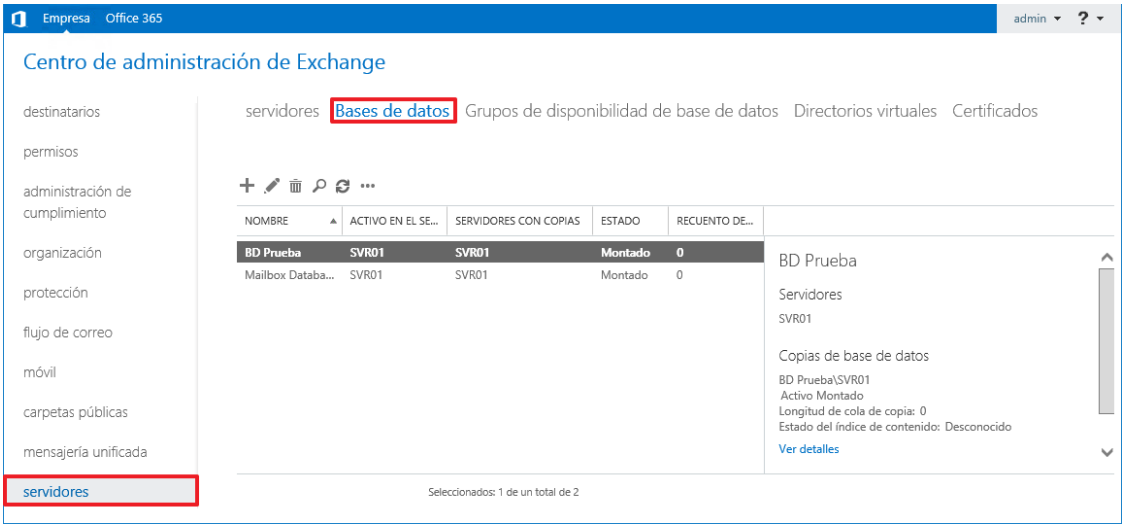
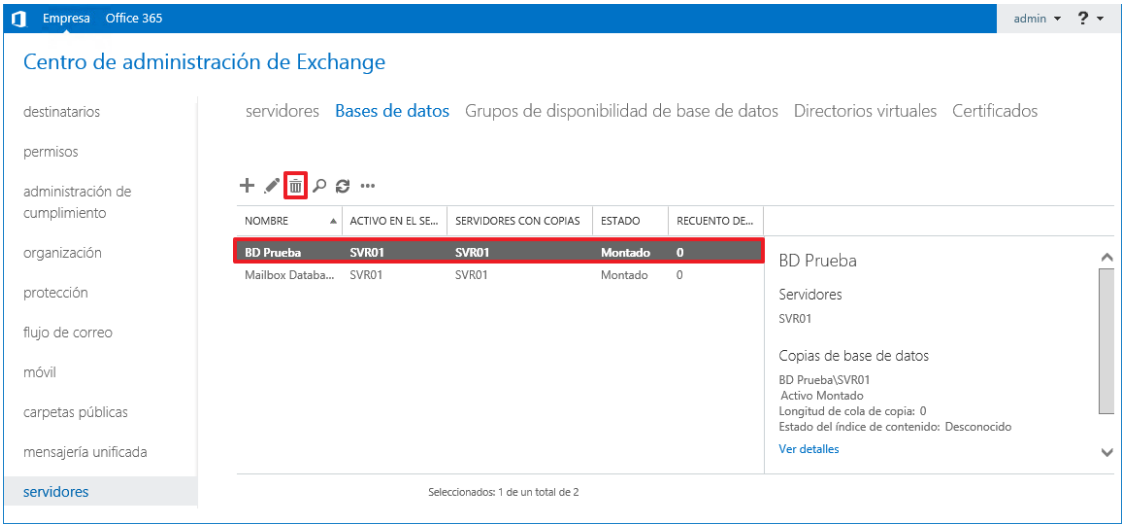
Un grupo de disponibilidad de base de datos (DAG) es un conjunto de hasta 16 servidores de buzones Microsoft Exchange Server 2016 que ofrece recuperación automática de base de datos a partir de un error de base de datos, servidor o red. Cuando un servidor de buzones se agrega a un DAG, funciona con los demás servidores del DAG para ofrecer recuperación automática de base de datos a partir de los errores de base de datos, servidor y red.

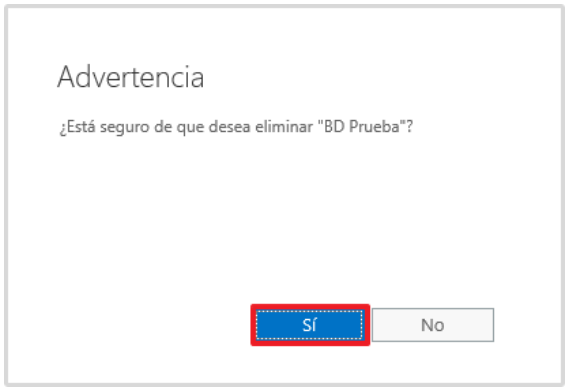
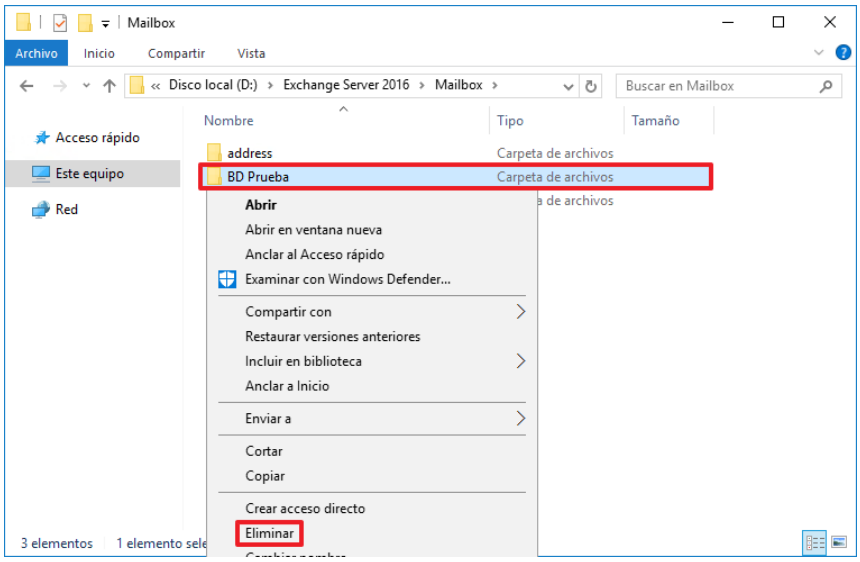
3.14. BORRADO SEGURO DE BASES DE DATOS

En Exchange Server 2016 edición Enterprise se pueden crear hasta 100 bases de datos por cada servidor de buzones, pudiendo alojar miles de buzones de usuarios en cada una de esas bases de datos. No existe un límite impuesto sobre el tamaño de las bases de datos y los buzones en Exchange Server 2016, aunque se recomienda que las bases de datos de buzones no superen los 200 GB para entornos no agrupados y de 2 TB para servidores de buzones en grupos de disponibilidad (DAG) con replicación habilitada.

A continuación, se detalla cómo eliminar una base de datos de buzones del servidor.

Paso	Descripción
162.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado Exchange Server 2016 con una cuenta con permisos de administrador. El acceso a la consola Web de administración de Exchange, se puede realizar desde cualquier equipo conectado a la red, aunque en este ejemplo se realizará desde el servidor miembro donde está instalado Exchange Server 2016.
163.	Pulse sobre "Internet Explorer" en la barra de tareas. 
164.	Introduzca la URL para acceder al "Exchange Administrative Center" de su organización.  **Nota:** En este ejemplo se usa la ruta "https://SVR01/ecp" donde "SVR01" es el nombre del servidor donde se encuentra instalado Exchange Server 2016.
165.	Inicie sesión en la consola Web con una cuenta con privilegios de administrador de la organización Exchange.  **Nota:** En este ejemplo se utiliza la cuenta "dominio\admin".

Paso	Descripción
166.	A continuación, diríjase a **"servidores → Bases de datos"**. 
167.	Seleccione la base de datos que desea eliminar y pulse sobre "Borrar".  **Nota:** Si existen buzones alojados en la base de datos que desea eliminar debería previamente mover los buzones a otra base de datos para que el sistema permita eliminar la base de datos. En este ejemplo se elimina la base de datos "BD Prueba".

Paso	Descripción
168.	Asegúrese que es correcta la base de datos que desea eliminar, y pulse "sí". 
169.	A continuación, le aparecerá una advertencia indicando que debe dirigirse a la ubicación física donde tenía alojada la base de datos y deberá eliminarla manualmente. Pulse "Aceptar" para cerrar la advertencia. 
170.	Diríjase a la ubicación de la base de datos, seleccione la base de datos que acaba de eliminar de la consola de administración de Exchange 2016 y elimine manualmente la carpeta de la base de datos.  **Nota:** El sistema le solicitará elevación de privilegios para acceder a la ruta donde se alojan las bases de datos.

3.15. CIFRADO DE LA INFORMACIÓN Y FIRMA ELECTRONICA

El ENS establece que la información con un nivel alto en confidencialidad debe estar cifrada para evitar con ello en caso de intercepción de la información emitida en un correo electrónico sea sustraída. Cada organización debe analizar la conveniencia de implantar controles y herramientas para el cifrado y firma del correo electrónico de acreditada robustez, que empleen algoritmos acreditados por el Centro Criptológico Nacional y preferentemente productos certificados en el caso de entornos de categoría alta – Difusión Limitada.

Exchange Server 2016 permite implementar mecanismos de cifrado y control de la información adicionales como S/MIME y derechos de información (IRM).

S/MIME permite cifrar mensajes de correo electrónico y firmarlos digitalmente. Cuando se usa S/MIME con un mensaje de correo electrónico, los destinatarios pueden comprobar que lo que ven en sus bandejas de entrada es el mensaje exacto que envió el remitente.

El cifrado es una forma de modificar información de manera que no se pueda leer o entender hasta que vuelva a cambiarse a un formato legible y entendible. El cifrado de mensajes ofrece dos servicios de seguridad específicos:

a) **Confidencialidad.** El cifrado de mensajes protege el contenido de un mensaje de correo electrónico. Sólo el destinatario al que va dirigido el mensaje puede ver el contenido, y el contenido sigue siendo confidencial y no puede conocerlo nadie más que quien pueda recibir o ver el mensaje.

b) **Integridad de los datos.** El cifrado de mensajes ofrece servicios de integridad de los datos como resultado de las operaciones específicas que hacen posible el cifrado.

Nota: Si desea obtener más información sobre la configuración de S/MIME puede visitar el siguiente sitio web:
https://technet.microsoft.com/es-es/library/dn626158(v=exchg.150).aspx

Las firmas digitales son el servicio más utilizado de S/MIME. Como su nombre indica, las firmas digitales son la contrapartida digital a la tradicional firma legal en un documento impreso. Al igual que ocurre con una firma legal, las firmas digitales ofrecen las diferentes capacidades de seguridad:

a) **Autenticación.** Una firma sirve para validar una identidad. Comprueba la respuesta a "quién es usted" al ofrecer una forma de diferenciar esa entidad de todas las demás y demostrar su unicidad. Como no existe autenticación en el correo electrónico SMTP, no hay ninguna forma de saber quién envió realmente un mensaje. La autenticación en una firma digital resuelve este problema al permitir que un destinatario sepa que un mensaje fue enviado por la persona o la organización que dice haber enviado el mensaje.

b) **No rechazo.** La unicidad de una firma impide que el propietario de la firma no reconozca su firma. Esta capacidad se llama no rechazo. Así, la autenticación proporcionada por una firma aporta el medio de exigir el no rechazo. El concepto de no rechazo resulta más familiar en el contexto de los contratos en papel: un contrato firmado es un documento legalmente vinculante y es imposible no reconocer una firma autenticada. Las firmas digitales ofrecen la misma función y, cada vez en más áreas, se reconocen como legalmente vinculantes, de manera similar a una firma en un papel. Como el correo electrónico SMTP no ofrece ningún medio de autenticación, no puede proporcionar la función de no rechazo. Para el remitente de un mensaje de correo electrónico SMTP es fácil no reconocer la propiedad del mismo.

c) **Integridad de los datos.** Un servicio de seguridad adicional que ofrecen las firmas digitales es la integridad de los datos. La integridad de los datos es uno de los resultados de las operaciones que hacen posibles las firmas digitales. Con los servicios de integridad de datos, cuando el destinatario de un mensaje de correo electrónico firmado digitalmente valida la firma digital, tiene la seguridad de que el mensaje recibido es el mismo mensaje que se firmó y se envió, y que no se ha manipulado mientras estaba en tránsito. Cualquier alteración del mensaje mientras estaba en tránsito una vez firmado invalida la firma. De esta forma, las firmas digitales son capaces de ofrecer una garantía que no permiten tener las firmas en papel, ya que es posible alterar un documento en papel una vez que ha sido firmado.

Nota: Aunque las firmas digitales ofrecen integridad de los datos, no proporcionan confidencialidad. Los mensajes que sólo tienen una firma digital se envían como texto no cifrado, de manera similar a los mensajes SMTP.

3.16. PROTECCIÓN DE DATOS Y RECUPERACIÓN DE ELEMENTOS ELIMINADOS

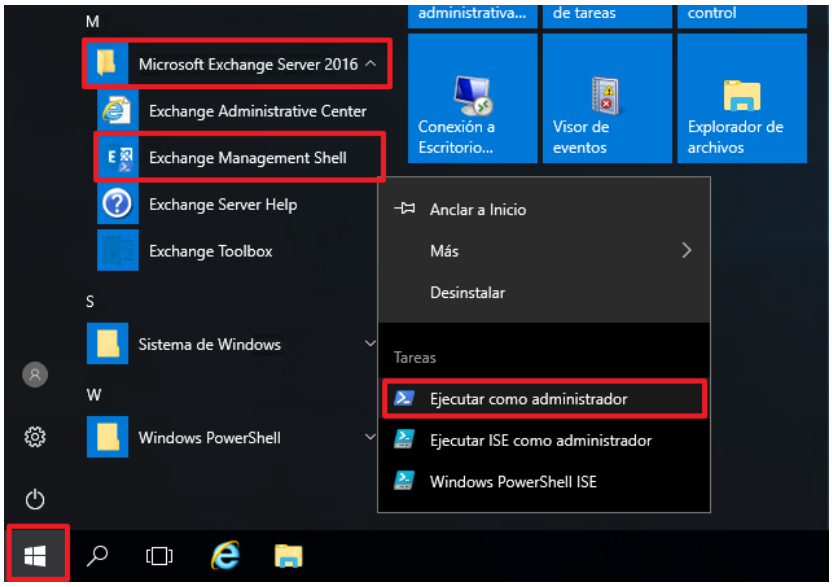
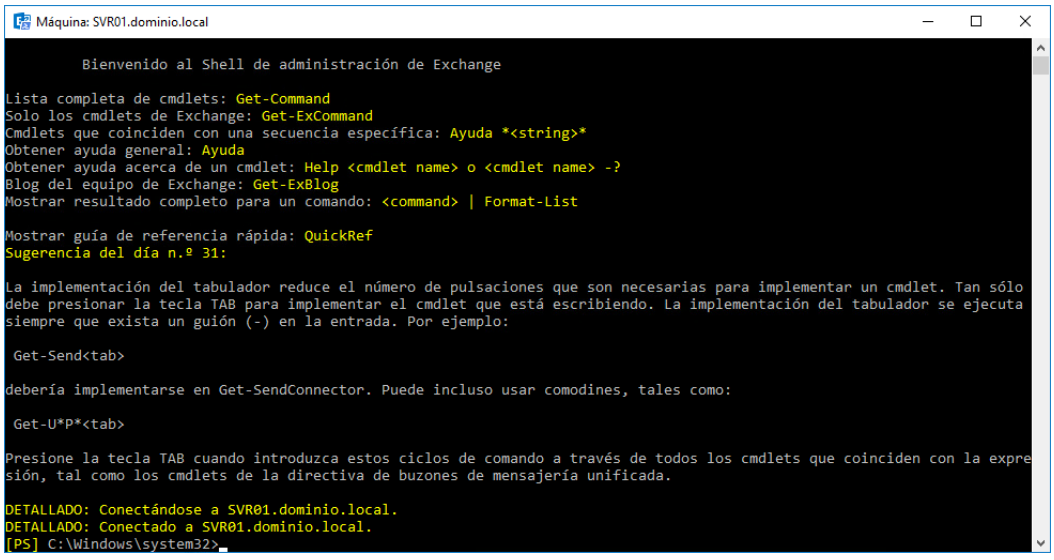
Microsoft para Exchange Server 2016 usa un concepto conocido como Exchange Native Data Protection, el cual se basa en características integradas de Exchange para proteger los datos de su buzón de correo sin tener que usar copias de seguridad (aunque puede seguir utilizando dichas características para crear copias de seguridad). Exchange 2016 incluye varias características nuevas y cambios generales que, una vez implementados y configurados correctamente, ofrecen una protección de datos nativa que elimina la necesidad de realizar copias de datos tradicionales.

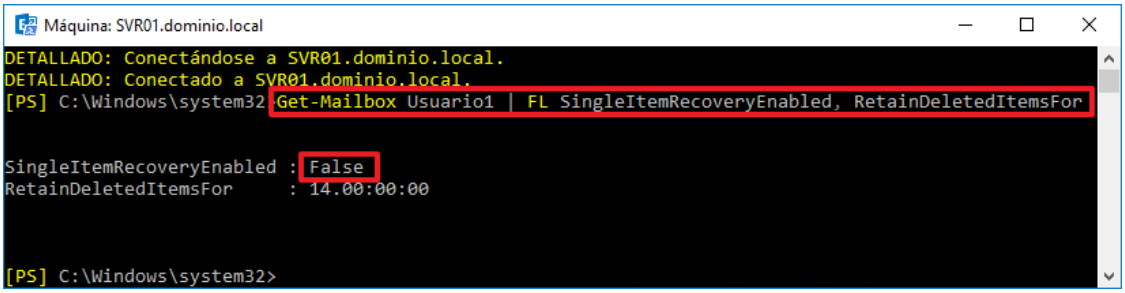
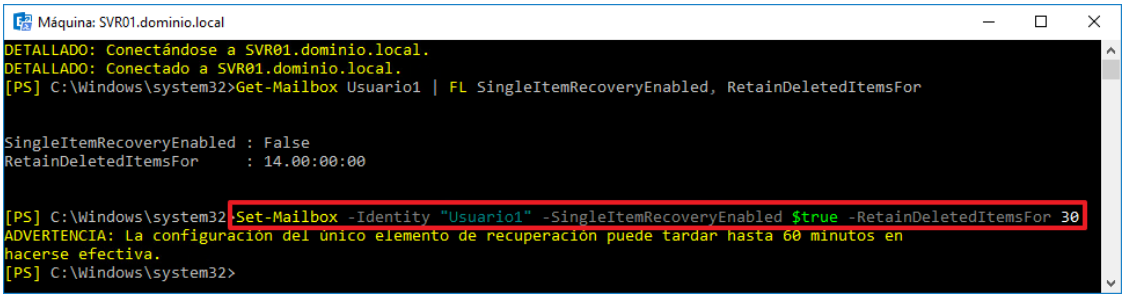
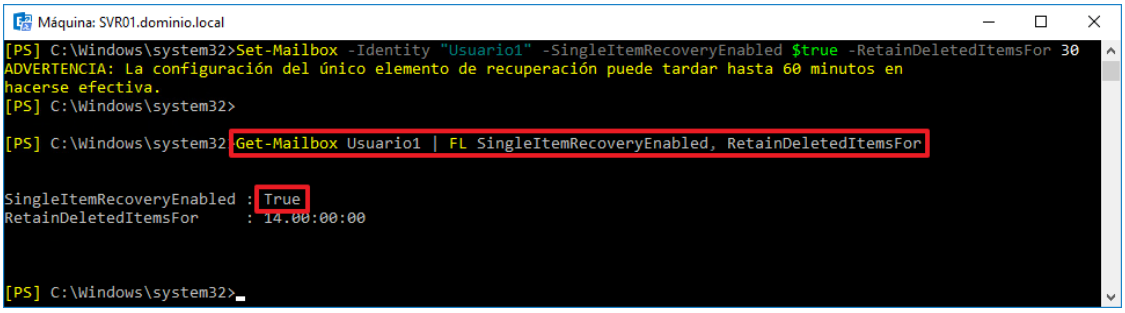
Exchange 2016 también implementa los grupos de disponibilidad de bases de datos (DAG). Un grupo de disponibilidad de base de datos (DAG) es el componente básico del marco de alta disponibilidad y resistencia de sitios del servidor de buzones que ofrece Microsoft Exchange Server 2016. Un DAG es un límite para la replicación de bases de datos de buzones, los cambios de bases de datos y de servidores, y las conmutaciones por error, así como para un componente interno denominado Active Manager.

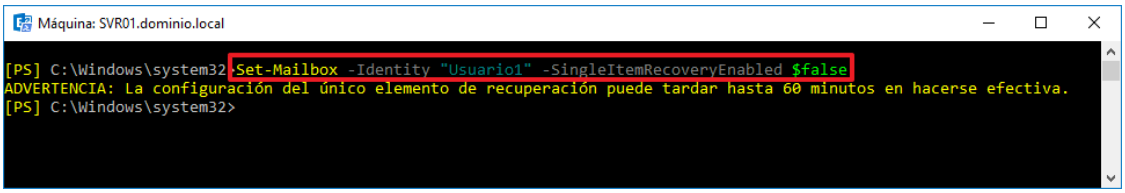
Cualquier servidor en un DAG puede hospedar una copia de una base de datos de buzones de correo de cualquier otro servidor en el DAG. Cuando se agrega un servidor a un DAG funciona con los otros servidores del DAG para proporcionar recuperación automática de errores que afectan a las bases de datos de buzones, como un error de disco, de servidor o de red.

Además, Microsoft Exchange Server 2016, también ofrece la recuperación de un elemento único la cual se deshabilita cuando se crea un buzón. Si la recuperación de un elemento único está habilitada, los mensajes que el usuario elimina (purga) permanentemente se conservan en la carpeta Elementos recuperables del buzón hasta que expira el período de retención de elementos eliminados. Esto permite al administrador recuperar los mensajes purgados por el usuario antes de que expire el período de retención de elementos eliminados.

A continuación, se muestra cómo habilitar la recuperación de un elemento único el cual viene deshabilitado por defecto.

Paso	Descripción
171.	Inicie sesión en el servidor miembro donde está instalado Microsoft Exchange Server 2016 con un usuario con permisos de administrador.
172.	Pulse sobre el menú inicio despliegue la carpeta "Microsoft Exchange Server 2016" y pulsando con botón derecho en "Exchange Management Shell" seleccione "Ejecutar como administrador".  **Nota:** El sistema le solicitará elevación de privilegios.
173.	A continuación, se mostrará la siguiente ventana. 

Paso	Descripción
174.	A continuación, si desea comprobar si está habilitada la recuperación ejecute el comando y compruebe que el estado es "False". – "Get-Mailbox <Nombre_buzon> | FL SingleItemRecoveryEnabled, RetainDeletedItemsFor" Sustituya "<Nombre_buzon>" por el nombre de buzón que desea comprobar. 
175.	A continuación, para habilitar la recuperación de elementos eliminados ejecute el siguiente comando. – "Set-Mailbox -Identity "Usuario1" -SingleItemRecoveryEnabled $true -RetainDeletedItemsFor 30" Además, se establecerá que el tiempo de conservación de los correos será de 30 días. 
176.	Compruebe que ha habilitado correctamente la recuperación de elementos eliminados. Ejecute nuevamente el siguiente comando. – "Get-Mailbox <Nombre_buzon> | FL SingleItemRecoveryEnabled, RetainDeletedItemsFor" Compruebe que el estado es "True". 

Paso	Descripción
177.	En caso de que desee deshabilitar la recuperación de elementos eliminados deberá ejecutar el comando. – "Set-Mailbox -Identity "Nombre_Usuario" -SingleItemRecoveryEnabled $false"  **Nota:** Si desea más información acerca de la recuperación de elementos eliminados en Exchange Server 2016 visite el sitio web: https://technet.microsoft.com/es-es/library/ee633460(v=exchg.150).aspx

3.17. PROTECCIÓN DE SERVICIOS

Exchange Server 2016 utiliza IIS por lo que todos los sistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que le competen como:

a) Ataques directos, tales como accesos no autorizados sobre cualquiera de los elementos que conforman el entorno.

b) Ataques indirectos, dónde cualquiera de los elementos es empleado como herramienta en el ataque.

c) Ataques de denegación de servicio (DoS). Las arquitecturas Web están basadas en tecnologías TCP/IP y por tanto son vulnerables a los ataques de DoS comunes en TCP/IP. Es necesario disponer de contramedidas técnicas y procedimientos de actuación frente a este tipo de ataques.

Para una mayor seguridad sobre Exchange Server 2016 se han de configurar los filtros de solicitudes los cuales permiten controlar las conexiones entre servidor y cliente, restringiendo el comportamiento de protocolos y contenidos.

Se considera una buena práctica de seguridad realizar una configuración básica para el servidor según los usos, situación, contenidos a servir, etc. que se le prevén y luego afinar aún más en cada uno de los sitios que se generen.

El filtro de solicitudes es un módulo, o servicio de rol, de IIS instalable (por medio de AppCMD.exe, Administrador del servidor, Powershell, etc.) de forma individual y configurable por cualquiera de los medios habituales (Administrador de Internet Information Services (IIS), AppCMD.exe, etc.).

En el apartado "2 PREPARACIÓN DEL IIS 10" se aplica seguridad sobre URLfiltering para Microsoft Exchange Server 2016.

ANEXO A.4.2. LISTA DE COMPROBACIÓN

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

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

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

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:

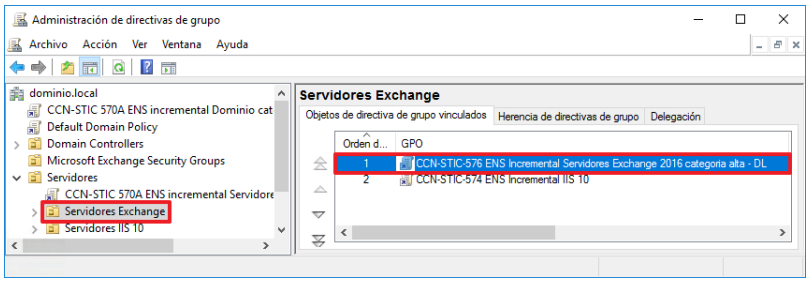
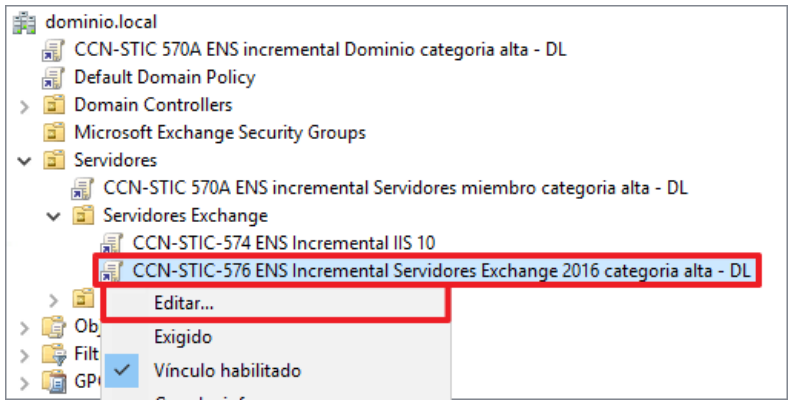
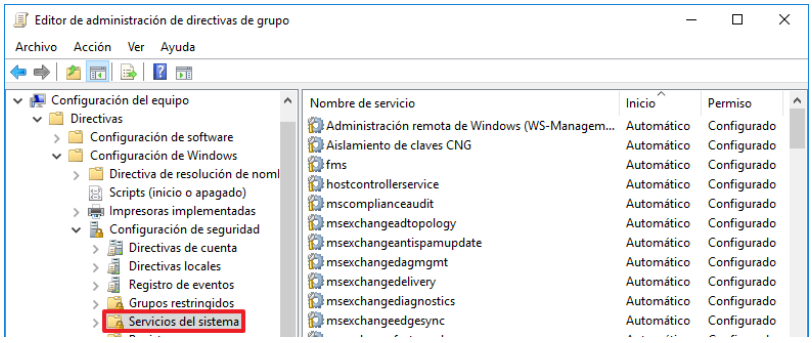
a) Usuarios y equipos de Active Directory (dsa.msc).

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

c) Editor de objetos de directiva de grupo (gpedit.msc).

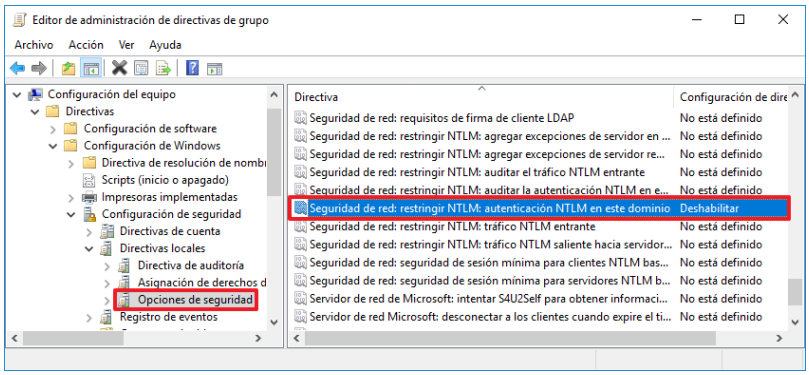
Nota: La lista de comprobación está basada en los nombres de objetos de directivas, unidades organizativas y cuentas de servicios tal y como se ha indicado durante la presente guía. Deberá adaptar los pasos según la configuración de su organización.

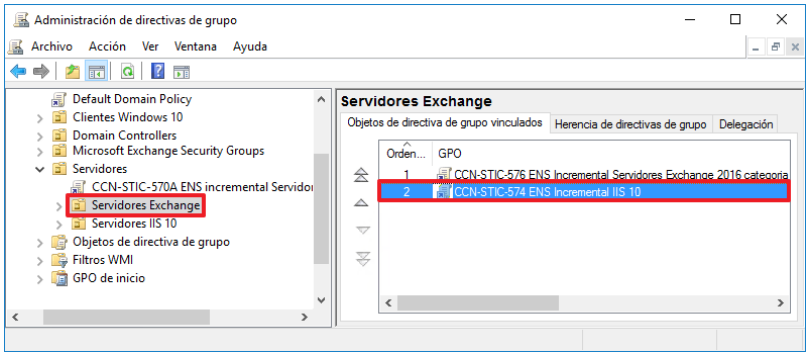
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
2. Verifique que está creada la directiva de Exchange 2016 (CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria alta - DL).		Ejecute la herramienta "Administración de directivas de grupo" desde "**Administrador del servidor → Herramientas → Administración de directivas de grupo**". El sistema le solicitará elevación de privilegios para acceder al administrador del servidor. Seleccione la unidad organizativa "Servidores Exchange", situada en **"Bosque → Dominios → [Su_dominio] → Servidores → Servidores Exchange"** y a continuación, en el panel de la derecha, verifique que está creado el objeto de directiva de grupo denominado "CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria alta - DL" y se encuentra en el primer orden de directivas de grupo vinculados.

Comprobación	OK/NOK	Cómo hacerlo
		 Seleccione con el botón derecho el objeto de directiva de grupo y haga clic en la opción "Editar" del menú para verificar los valores de la directiva "CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria alta - DL". 
3. Verifique los valores de los servicios del sistema de la directiva CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria alta - DL.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria alta – DL" tiene los siguientes valores de servicios de sistema. **"Directiva CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria alta - DL→ Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema".**  **Nota:** Puede ordenar los servicios por la columna "Inicio". Dependiendo de los servicios que estén instalados en el controlador de dominio utilizado para la verificación, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales. Cuando finalice, cierre el editor de objetos de directiva de grupo.

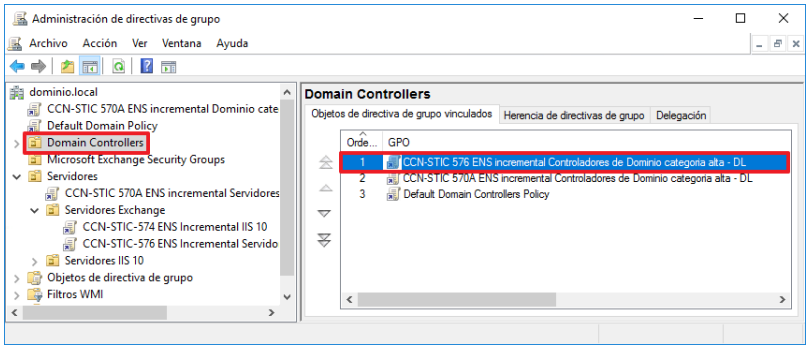
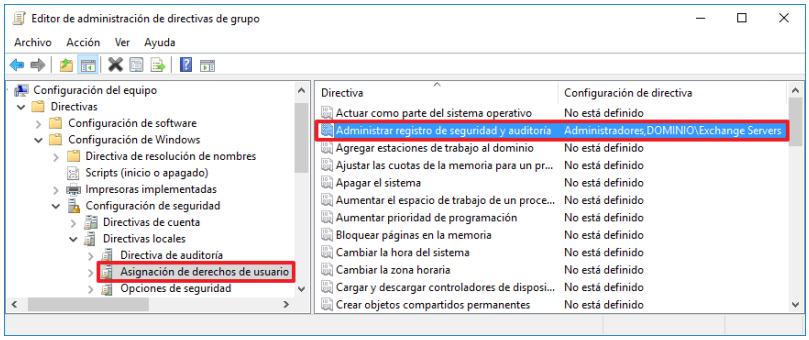
Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permisos**	**OK/NOK**	
Actualización de correo no deseado de Microsoft Exchange	msexchangeantispamupdate	Automático	Configurado		
Administración de Microsoft Exchange DAG	msexchangedagmgmt	Automático	Configurado		
Administración remota de Windows (WS-Management)	Winrm	Automático	Configurado		
Administrador del estado de Microsoft Exchange	msexchangehm	Automático	Configurado		
Aislamiento de claves CNG	keyiso	Automático	Configurado		
Asistentes de buzón de Microsoft Exchange	msexchangemailboxassistants	Automático	Configurado		
ASP.NET State Service	aspnet_state	Manual	Configurado		
Host de servicios de cumplimiento de normas.	msexchangecompliance	Automático	Configurado		
Auditoría de conformidad de Microsoft Exchange	mscomplianceaudit	Automático	Configurado		
Back- end POP3 de Microsoft de Microsoft Exchange	msexchangepop3be	Deshabilitado	Configurado		
Back-end IMAP 4 de Microsoft Exchange	msexchangeimap4be	Deshabilitado	Configurado		
Búsqueda de Microsoft Exchange	msexchangefastsearch	Automático	Configurado		
Diagnósticos de Microsoft Exchange	msexchangediagnostics	Automático	Configurado		
Enrutador de llamadas de mensajería unificada de Microsoft Exchange	msexchangeumcr	Automático	Configurado		
Entrega de transporte de buzones de Microsoft Exchange	msexchangedelivery	Automático	Configurado		
Envío de transporte de buzones de Microsoft Exchange	msexchangesubmission	Automático	Configurado		
Límite de Microsoft Exchange	msexchangethrottling	Automático	Configurado		
Mensajería unificada de Microsoft Exchange	msexchangeum	Automático	Configurado		
Microsoft Exchange EdgeSync	msexchangeedgesync	Automático	Configurado		
Microsoft Exchange IMAP4	msexchangeimap4	Deshabilitado	Configurado		
Microsoft Exchange Information Store	msexchangeis	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permisos**	**OK/NOK**	
Microsoft Exchange Notifications Broker	msexchangenotificationsbroker	Automático	Configurado		
Microsoft Exchange POP3	msexchangepop3	Deshabilitado	Configurado		
Microsoft Exchange Search Host Controller	hostcontrollerservice	Automático	Configurado		
Microsoft Exchange Server Extension for Windows Server Backup	wsbexchange	Manual	Configurado		
Microsoft Exchange Service Host	msexchangeservicehost	Automático	Configurado		
Notificaciones del servicio de token de Windows	c2wts	Manual	Configurado		
Recuperación del administrador del estado de Microsoft Exchange	msexchangehmrecovery	Automático	Configurado		
Registro de búsquedas de Transport de Microsoft Exchange	msexchangetransportlogsearch	Automático	Configurado		
Registro remoto	remoteregistry	Automático	Configurado		
Replicación de buzón de Microsoft Exchange	msexchangemailboxreplication	Automático	Configurado		
Replicación de Microsoft Exchange	msexchangerepl	Automático	Configurado		
Servicio de acceso de cliente RPC de Microsoft Exchange	msexchangerpc	Automático	Configurado		
Servicio de administración de filtrado de Microsoft	fms	Automático	Configurado		
Servicio de equilibrio de carga RPC/HTTP	rpchttplbs	Manual	Configurado		
Servicio de uso compartido de puertos Net.Tcp	nettcpportsharing	Automático	Configurado		
Servicio WAS (Windows Process Activation Service)	was	Automático	Configurado		
Servidor	lanmanserver	Automático	Configurado		
Sistema de eventos COM+	eventsystem	Manual	Configurado		
Topología de Active Directory de Microsoft Exchange	msexchangeadtopology	Automático	Configurado		
Tracing Service for Search in Exchange	searchexchangetracing	Automático	Configurado		
Transport de Microsoft Exchange	msexchangetransport	Automático	Configurado		
Transporte Frontend de Microsoft Exchange	msexchangefrontendtransport	Automático	Configurado		

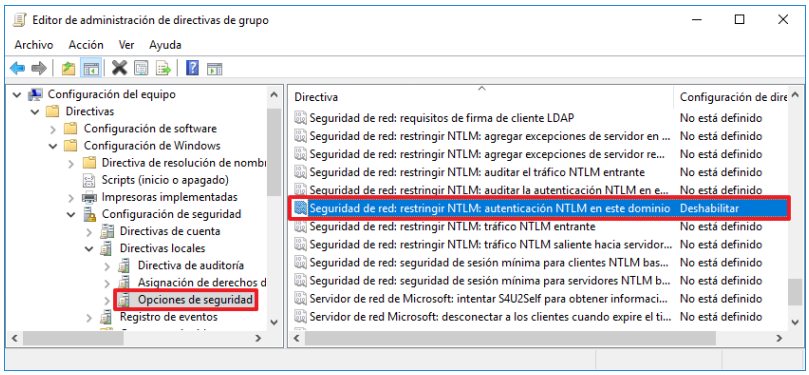
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>4. Verifique los valores de las opciones de seguridad de la directiva CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria alta - DL.</td><td></td><td>Utilizando el editor de objetos de directiva de grupo, verifique que la directiva “CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria alta – DL” tiene los siguientes valores de servicios de sistema.
“Directiva CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria alta - DL→ Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 

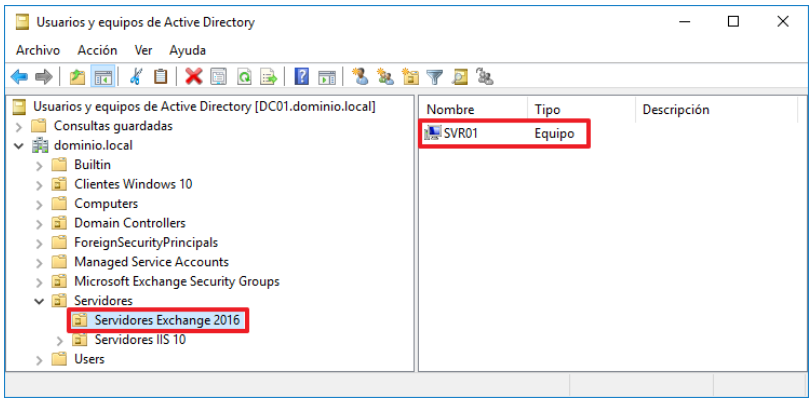
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Seguridad de red: restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitar</td><td></td></tr>
</table></td></tr>
<tr><td>5. Verifique que está creada la directiva de Internet Information Services 10 (CCN-STIC-574 ENS Incremental IIS 10).</td><td></td><td>En la consola “Administración de directivas de grupo”, seleccione la unidad organizativa “Servidores Exchange”, situada en “Bosque → Dominios → [Su_dominio] → Servidores → Servidores Exchange” y a continuación, verifique que está creado el objeto de directiva de grupo denominado “CCN-STIC-574 ENS Incremental IIS 10”.
 

Nota: La configuración de seguridad de esta GPO deberá de haberse comprobado en la guía codificada como “CCN-STIC-574”.</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>6. Verifique que está creada la directiva CCN-STIC-576 ENS Incremental Controladores de Dominio Exchange categoria alta - DL.</td><td></td><td>Sin salir de la consola “Administración de directivas de grupo”, seleccione la unidad organizativa “Servidores Exchange”, situada en “Bosque → Dominios → [Su_dominio] → Domain Controllers” y a continuación, verifique que está creado el objeto de directiva de grupo denominado “CCN-STIC-576 ENS Incremental Controladores de Dominio Exchange categoria alta - DL” y se encuentra en el primer orden de vínculos.
 
</td></tr>
<tr><td>7. Verifique los valores de seguridad de la directiva CCN-STIC-576 ENS Incremental Controladores de Dominio Exchange categoria alta - DL.</td><td></td><td>Utilizando el editor de objetos de directiva de grupo, verifique que la directiva “CCN-STIC-576 ENS Incremental Controlador de Dominio Exchange categoria alta - DL” tiene el siguiente valor de seguridad.
“CCN-STIC-576 ENS Incremental Controladores de Dominio Exchange categoria alta - DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Administrar registro de seguridad y auditoría</td><td>Administradores Exchange Servers</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>8. Verifique los valores de las opciones de seguridad de la directiva CCN-STIC-576 ENS Incremental Controladores de Dominio Exchange categoria alta - DL.</td><td></td><td>Utilizando el editor de objetos de directiva de grupo, verifique que la directiva “CCN-STIC-576 ENS Incremental Controladores de Dominio Exchange categoria alta - DL” tiene los siguientes valores de servicios de sistema.
“Directiva CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria alta - DL→ Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Seguridad de red: restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitar</td><td></td></tr>
</table></td></tr>
<tr><td>9. Verifique que los servidores a asegurar están dentro de la unidad organizativa “Servidores Exchange”.</td><td></td><td>Ejecute la herramienta “Usuarios y equipos de Active Directory” desde “Administrador del servidor → Herramientas → Usuarios y equipos de Active Directory”. El sistema le solicitará elevación de privilegios para acceder al administrador del servidor.
A continuación, seleccione la unidad organizativa “Servidores Exchange” y verifique que se encuentra el servidor donde se ha instalado Exchange Server 2016.
 
</td></tr>
</table>

2. COMPROBACIONES EN SERVIDOR MIEMBRO

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:

a) Administrador de Windows (explorer.exe).

b) Símbolo del sistema (cmd.exe).

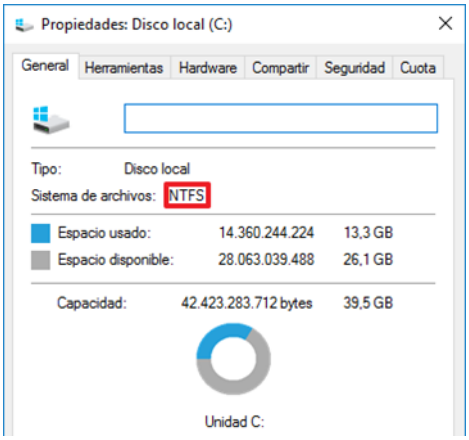
c) Servicios (services.msc).

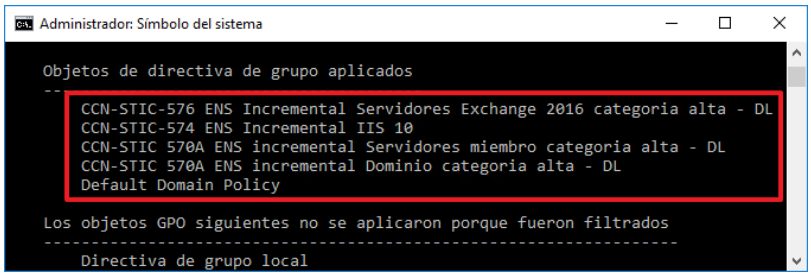
d) Editor de objetos de directiva de grupo (gpedit.msc).

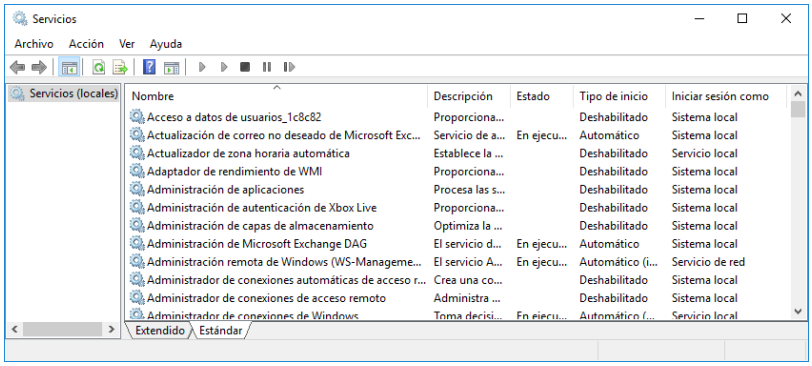
e) Administrador de Internet Information Services (iis.msc).

f) Consola Web de administración de Exchange 2016.

g) Shell de administración de Exchange 2016.

Comprobación	OK/NOK	Cómo hacerlo
10. Inicie sesión en los servidores Exchange 2016.		A continuación, para completar el resto de la lista de comprobación deberá iniciar sesión en el servidor donde se aloja Exchange Server 2016 con una cuenta que tenga permisos de administrador local del servidor, administrador del dominio o administrador de la organización de Exchange.
11. Verifique que todos los volúmenes están formateados con NTFS.		Utilizando el explorador de Windows (botón derecho sobre **Inicio → Explorador de archivos, botón derecho sobre la unidad C:\ → Propiedades**), verifique en las propiedades de cada partición el uso del sistema de archivos NTFS o cualquier sistema de archivos que permita ACL's. 

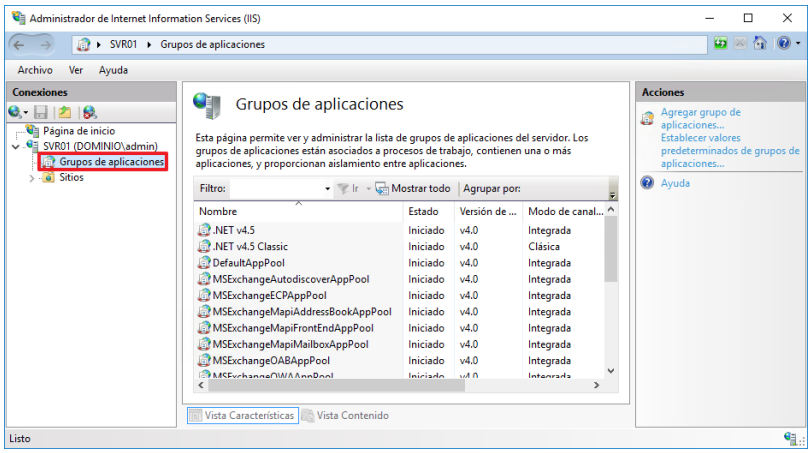
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>12. Verifique que le están aplicando las GPO de forma correcta.</td><td></td><td>Abra una consola de comandos como administrador con botón derecho en “Inicio → Símbolo del sistema (administrador)” y ejecute el comando “gpresult –r”. Compruebe que las GPO están aplicando al equipo en el orden correcto.
 

<table>
<tr><th>Objeto de directiva de grupo</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-576 ENS Incremental Servidores Exchange 2016 categoria alta - DL</td><td></td></tr>
<tr><td>CCN-STIC-574 ENS Incremental IIS 10</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS Incremental Dominio categoria alta - DL</td><td></td></tr>
<tr><td>Default Domain Policy</td><td></td></tr>
</table></td></tr>
<tr><td>13. Verifique que los servicios del sistema están configurados de forma correcta.</td><td></td><td>Ejecute la herramienta “Servicios” desde “Administrador del servidor → Herramientas → Servicios”. El sistema le solicitará elevación de privilegios para acceder al administrador del servidor.
 

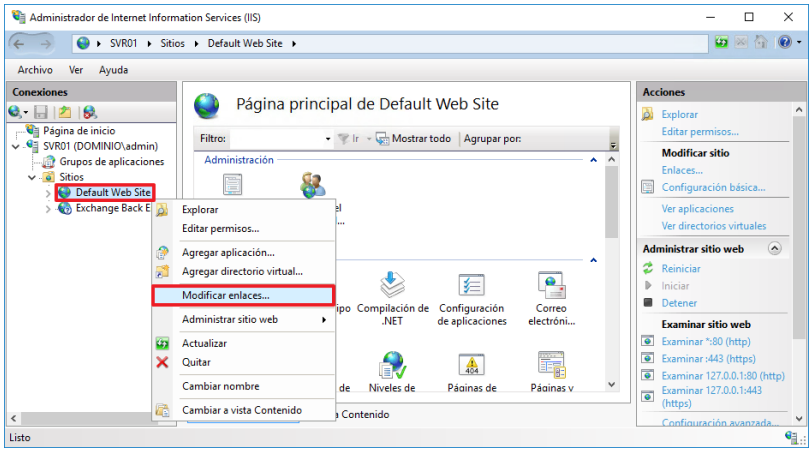
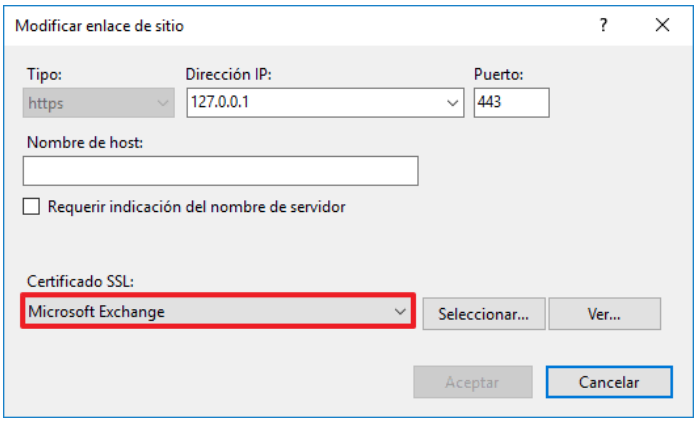
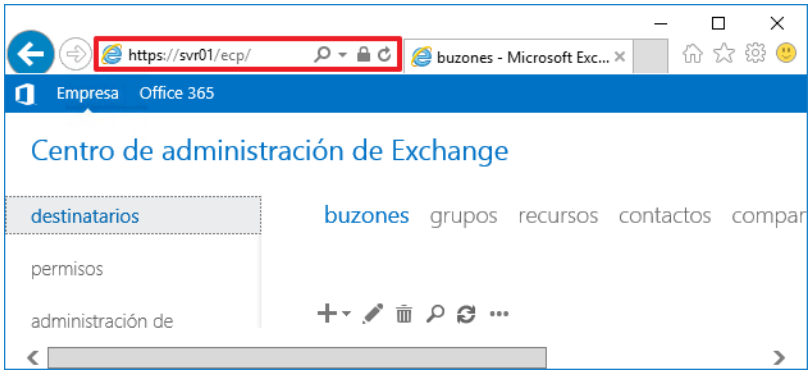
Nota: Dependiendo del equipo, es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales. Puede ordenar los servicios por “Tipo de inicio”. Sólo se verifican los servicios que configura esta guía.</td></tr>
</table>

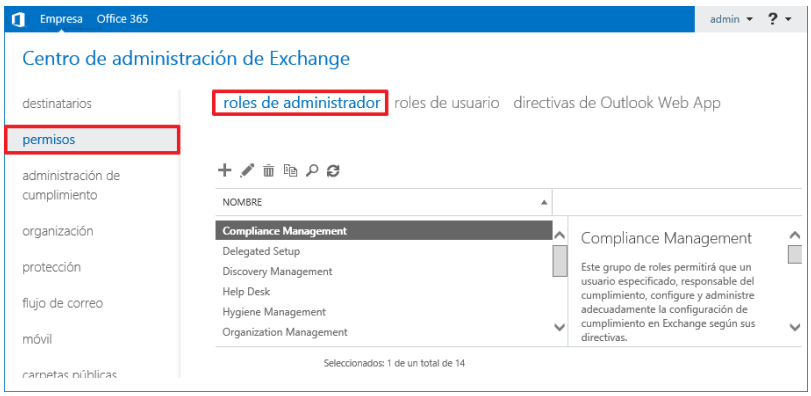
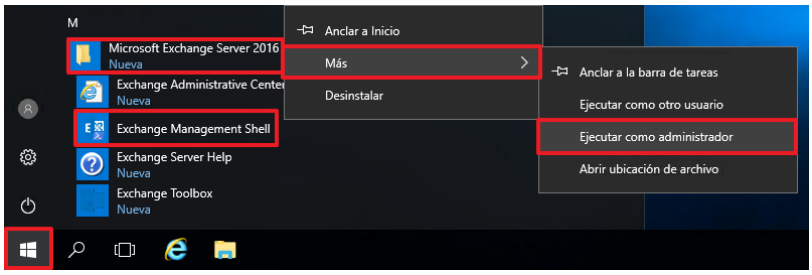
Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permisos**	**OK/NOK**	
Actualización de correo no deseado de Microsoft Exchange	msexchangeantispamupdate	Automático	Configurado		
Administración de Microsoft Exchange DAG	msexchangedagmgmt	Automático	Configurado		
Administración remota de Windows (WS-Management)	winrm	Automático	Configurado		
Administrador del estado de Microsoft Exchange	msexchangehm	Automático	Configurado		
Aislamiento de claves CNG	keyiso	Automático	Configurado		
Asistentes de buzón de Microsoft Exchange	msexchangemailboxassistants	Automático	Configurado		
ASP.NET State Service	aspnet_state	Manual	Configurado		
Auditoría de conformidad de Microsoft Exchange	mscomplianceaudit	Automático	Configurado		
Servicio de cumplimiento de normas de Microsoft Exchange.	msexchangecompliance	Automático	Configurado		
Back- end POP3 de Microsoft de Microsoft Exchange	msexchangepop3be	Deshabilitado	Configurado		
Back-end IMAP 4 de Microsoft Exchange	msexchangeimap4be	Deshabilitado	Configurado		
Búsqueda de Microsoft Exchange	msexchangefastsearch	Automático	Configurado		
Diagnósticos de Microsoft Exchange	msexchangediagnostics	Automático	Configurado		
Enrutador de llamadas de mensajería unificada de Microsoft Exchange	msexchangeumcr	Automático	Configurado		
Entrega de transporte de buzones de Microsoft Exchange	msexchangedelivery	Automático	Configurado		
Envío de transporte de buzones de Microsoft Exchange	msexchangesubmission	Automático	Configurado		
Límite de Microsoft Exchange	msexchangethrottling	Automático	Configurado		
Mensajería unificada de Microsoft Exchange	msexchangeum	Automático	Configurado		
Microsoft Exchange EdgeSync	msexchangeedgesync	Automático	Configurado		
Microsoft Exchange IMAP4	msexchangeimap4	Deshabilitado	Configurado		
Microsoft Exchange Information Store	msexchangeis	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	**Servicio (nombre corto)**	**Inicio**	**Permisos**	**OK/NOK**	
Microsoft Exchange Notifications Broker	msexchangenotificationsbroker	Automático	Configurado		
Microsoft Exchange POP3	msexchangepop3	Deshabilitado	Configurado		
Microsoft Exchange Search Host Controller	hostcontrollerservice	Automático	Configurado		
Microsoft Exchange Server Extension for Windows Server Backup	wsbexchange	Manual	Configurado		
Microsoft Exchange Service Host	msexchangeservicehost	Automático	Configurado		
Notificaciones del servicio de token de Windows	c2wts	Manual	Configurado		
Recuperación del administrador del estado de Microsoft Exchange	msexchangehmrecovery	Automático	Configurado		
Registro de búsquedas de Transport de Microsoft Exchange	msexchangetransportlogsearch	Automático	Configurado		
Registro remoto	remoteregistry	Automático	Configurado		
Replicación de buzón de Microsoft Exchange	msexchangemailboxreplication	Automático	Configurado		
Replicación de Microsoft Exchange	msexchangerepl	Automático	Configurado		
Servicio de acceso de cliente RPC de Microsoft Exchange	msexchangerpc	Automático	Configurado		
Servicio de administración de filtrado de Microsoft	fms	Automático	Configurado		
Servicio de equilibrio de carga RPC/HTTP	rpchttplbs	Manual	Configurado		
Servicio de uso compartido de puertos Net.Tcp	nettcpportsharing	Automático	Configurado		
Servicio WAS (Windows Process Activation Service)	was	Automático	Configurado		
Servidor	lanmanserver	Automático	Configurado		
Sistema de eventos COM+	eventsystem	Manual	Configurado		
Topología de Active Directory de Microsoft Exchange	msexchangeadtopology	Automático	Configurado		
Tracing Service for Search in Exchange	searchexchangetracing	Automático	Configurado		
Transport de Microsoft Exchange	msexchangetransport	Automático	Configurado		
Transporte Frontend de Microsoft Exchange	msexchangefrontendtransport	Automático	Configurado		

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>14. En el servidor Exchange, verifique que se han creado los grupos de aplicaciones correspondientes.</td><td></td><td>Ejecute la herramienta “Administrador de Internet Information Services (IIS)” desde “Administrador del servidor → Herramientas → Administrador de Internet Information Services (IIS)”. El sistema le solicitará elevación de privilegios para acceder al administrador del servidor.
Seleccione el nodo “Nombre_Servidor → Grupo de aplicaciones” y verifique que existen los siguientes grupos de aplicaciones de Exchange.
 

<table>
<tr><th>Grupos de aplicaciones</th><th>OK/NOK</th></tr>
<tr><td>.Net v4.5</td><td></td></tr>
<tr><td>.Net v4.5 Classic</td><td></td></tr>
<tr><td>DefaultAppPool</td><td></td></tr>
<tr><td>MSExchangeAutodiscoverAppPool</td><td></td></tr>
<tr><td>MSExchangeECPAppPool</td><td></td></tr>
<tr><td>MSExchangeMAPIAddressBookAppPool</td><td></td></tr>
<tr><td>MSExchangeMAPIFrontEndAppPool</td><td></td></tr>
<tr><td>MSExchangeMAPIMailboxAppPool</td><td></td></tr>
<tr><td>MSExchangeOABAppPool</td><td></td></tr>
<tr><td>MSExchangeOWAAppPool</td><td></td></tr>
<tr><td>MSExchangeOWACalendarAppPool</td><td></td></tr>
<tr><td>MSExchangePowerShellAppPool</td><td></td></tr>
<tr><td>MSExchangePowerShellFrontEndAppPool</td><td></td></tr>
<tr><td>MSExchangePushNotificationsAppPool</td><td></td></tr>
<tr><td>MSExchangeRestAppPool</td><td></td></tr>
<tr><td>MSExchangeRestFrontEndAppPool</td><td></td></tr>
<tr><td>MSExchangeRPCProxyAppPool</td><td></td></tr>
<tr><td>MSExchangeRPCProxyFrontEndAppPool</td><td></td></tr>
<tr><td>MSExchangeServicesAppPool</td><td></td></tr>
<tr><td>MSExchangeSyncAppPool</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
15. En el servidor Exchange, verifique que se ha establecido el certificado correspondientes.		En la herramienta "Administrador de Internet Information Services (IIS)" seleccione con botón derecho el nodo **"Nombre_Servidor → Sitios → Default Web Site"** y pulse sobre "Modificar enlaces…".  Confirme que está seleccionado el certificado SSL correcto en el enlace de tipo https con puerto 443. 
16. Verifique el acceso la consola Web de Exchange Server 2016 se realiza de forma correcta.		Inicie sesión en la consola de administración de Exchange desde el navegador.  **Nota:** En este ejemplo se usa https://SVR01/ecp.

Comprobación	OK/NOK	Cómo hacerlo
17. Confirme que se ha creado un grupo de auditoría.		Pulse en **"Permisos → roles de administrador"** y confirme que se han aplicado los permisos adecuados a su organización. 
18. En el servidor Exchange, verifique el acceso correcto al Shell de Exchange Server 2016.		Inicie sesión en el Shell de administración de Exchange desde el menú **"Inicio → Todas las aplicaciones → Microsoft Exchange Server 2016"** y pulse con botón derecho en "Exchange Management Shell". El sistema le solicitará elevación de privilegios.  Tras introducir las credenciales, compruebe que se ejecute "Exchange Management Shell" correctamente como aparece en la siguiente imagen.