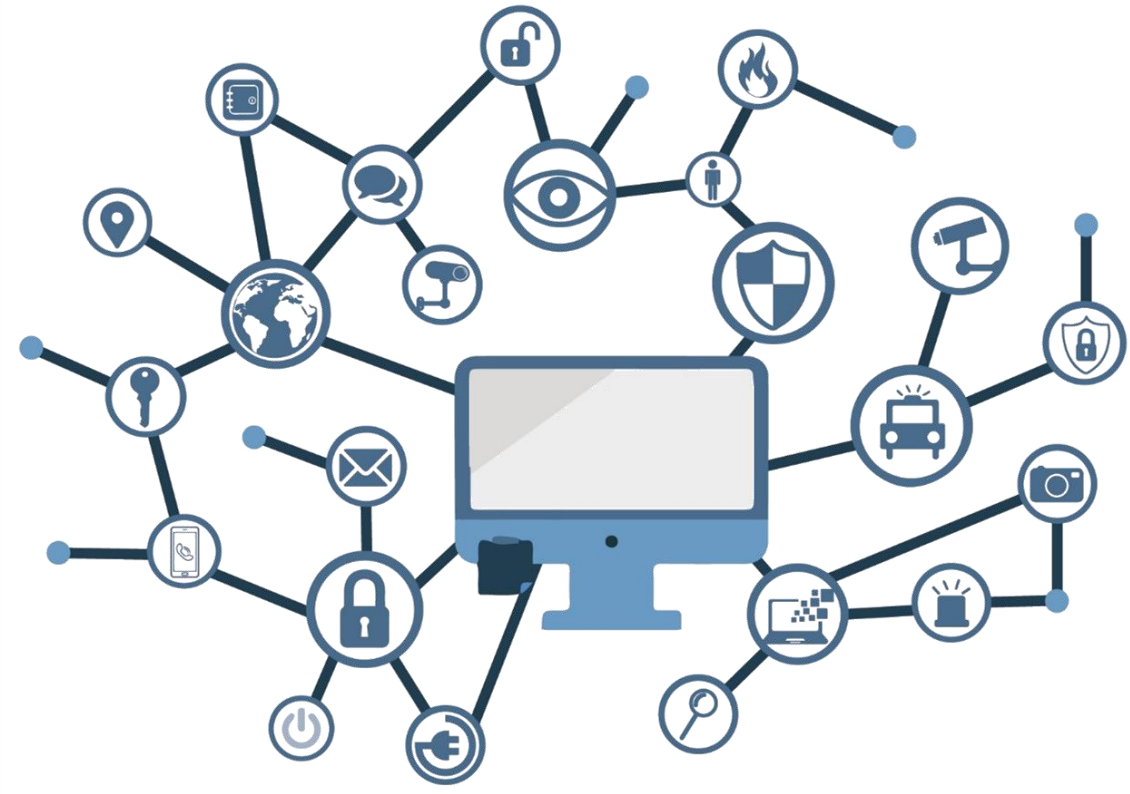
CCN
centro criptológico nacional

Guía de Seguridad de las TIC

MICROSOFT EXCHANGE SERVER 2016 EN 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.

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

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL 6
2. INTRODUCCIÓN 6
3. OBJETO 7
4. ALCANCE 8
5. DESCRIPCIÓN DEL USO DE ESTA GUÍA 9
5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA 9
5.2 ESTRUCTURA DE LA GUÍA 11
6. SEGURIDAD EN EXCHANGE SERVER 2016 11
6.1 MÉTODOS RECOMENDADOS PARA INSTALAR Y MANTENER UN ENTORNO DE EXCHANGE SERVER 2016 MÁS SEGURO 22
6.2 RELACIÓN DE PUERTOS, MECANISMOS DE AUTENTICACIÓN Y CIFRADO PARA LAS RUTAS DE DATOS ENTRE SERVIDORES EXCHANGE 2016 24
6.2.1 PUERTOS DE RED NECESARIOS PARA CLIENTES Y SERVICIOS 28
6.2.2 PUERTOS DE RED NECESARIOS PARA EL FLUJO DE CORREO 29
6.2.3 PUERTOS DE RED NECESARIOS PARA EL FLUJO DE CORREO CON SERVIDORES DE TRANSPORTE PERIMETRAL 30
6.2.4 SERVICIOS DE EXCHANGE SERVER 2016 32
6.3 SEGURIDAD DE DOMINIOS Y AUTENTICACIÓN MUTUA TLS 40
6.4 FILTRADO DE TRANSPORTE Y AGENTES DE CONFORMIDAD 41
6.4.1 AGENTE DE FILTRO DE CONEXIÓN 51
6.4.2 AGENTE DE FILTRO DE REMITENTES 51
6.4.3 AGENTE DE FILTRO DE DESTINATARIOS 52
6.4.4 AGENTE DE FILTRO DE IDENTIFICACIÓN DE REMITENTE 53
6.4.5 AGENTE DE FILTRO DE CONTENIDO 55
6.4.6 AGENTE DE ANÁLISIS DE PROTOCOLO Y REPUTACIÓN DE REMITENTE 60
6.4.7 AGENTE DE FILTRO DE DATOS ADJUNTOS 62
6.4.8 ANÁLISIS FRENTE A CÓDIGO DAÑINO 64
6.4.9 FILTRO DE CORREO ELECTRÓNICO NO DESEADO DE OUTLOOK 65
6.5 CUARENTENA DE EXCHANGE SERVER 2016 65
6.5.1 MARCAS DE CORREO NO DESEADO 66
6.6 CUENTA ADMINISTRATIVA DE INSTALACIÓN 69
6.7 PERMISOS 71
6.7.1 GRUPOS DE FUNCIONES DE ADMINISTRACIÓN 73
6.7.2 DIRECTIVAS DE ASIGNACIÓN DE ROLES DE ADMINISTRACIÓN 77
6.7.3 ASIGNACIONES DE FUNCIONES DE DELEGACIÓN 80
6.7.4 AMBITOS EXCLUSIVOS 80

6.7.5 TIPOS DE FUNCIONES DE ADMINISTRACIÓN 81
7. AUDITORÍA Y CONFORMIDAD 92
7.1 REGLAS DE FLUJO DE CORREO 93
7.1.1 CONDICIONES DE LAS REGLAS DE FLUJO DE CORREO 100
7.1.2 ACCIONES DE LAS REGLAS DE FLUJO DE CORREO 108
7.2 REGISTRO EN DIARIO 111
7.3 ADMINISTRACIÓN DE REGISTRO DE MENSAJES 114
7.4 EXHIBICIÓN DE DOCUMENTOS ELECTRÓNICOS EN CONTEXTO 117
7.5 CONSERVACIÓN LOCAL Y RETENCIÓN POR JUICIO 123
7.6 REGISTRO DE AUDITORÍA DE BUZÓN 126
7.7 CLASIFICACIÓN DE MENSAJES 130
7.8 ARCHIVO LOCAL 133
7.9 PREVENCIÓN DE PÉRDIDA DE DATOS (DLP) 137
7.10 INFORMATION RIGHTS MANAGEMENT (IRM) 139
7.10.1 PROTECCIÓN AUTOMÁTICA MEDIANTE REGLAS DE TRANSPORTE 142
7.10.2 PROTECCIÓN AUTOMÁTICA DE IRM EN OUTLOOK 143
7.11 S/MIME 144
7.12 REGISTRO DE AUDITORÍA DE ADMINISTRADOR 147

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en los productos y sistemas operativos de Microsoft (CCN STIC 500), siendo de aplicación para la Administración pública en el cumplimiento del Esquema Nacional de Seguridad (ENS) y de obligado cumplimiento para los sistemas que manejen información clasificada nacional.

La serie CCN-STIC-500 se ha diseñado de manera incremental. Así que, dependiendo del sistema, se aplicarán consecutivamente varias de estas guías. En este sentido se deberán aplicar las guías correspondientes dependiendo del entorno que se esté asegurando.

Por ejemplo, en el caso de un entorno que le sea de aplicación el ENS, para un servidor miembro de un dominio con Microsoft Windows Server 2012 R2, en el que se instale Microsoft Exchange Server 2013, deberán aplicarse las siguientes guías:

a) Guía CCN STIC 870A en el servidor miembro con Windows Server 2012 R2.

b) Guía CCN-STIC-873 Internet Information Services (IIS) 8.5.

c) Guía CCN STIC 880 Microsoft Exchange Server 2013 en Windows 2012 R2.

Por ejemplo, en el caso de un entorno de red clasificada, para un servidor con Microsoft Windows Server 2012 R2, en el que se instale Microsoft Exchange Server 2013, deberán aplicarse las siguientes guías:

a) Guía CCN STIC 560A en el servidor miembro con Windows Server 2012 R2.

b) Guía CCN-STIC-563 Internet Information Services (IIS) 8.5.

c) Guía CCN STIC 552 Microsoft Exchange Server 2013 en Windows 2012 R2.

Nota: Las guías que son de aplicación para entornos de red clasificada están pensadas y diseñadas para entornos de máxima seguridad donde no existirá conexión con redes no seguras como puede ser Internet.

3. OBJETO

El propósito de este documento consiste en proporcionar los procedimientos para implementar y garantizar la seguridad para una instalación completa del sistema de correo electrónico y colaboración "Exchange Server 2016" en su versión Standard o Enterprise en un servidor miembro de una infraestructura de dominio.

La configuración que se aplica a través de la presente guía se ha diseñado para ser lo más restrictiva posible, minimizando la superficie de ataque y por lo tanto los riesgos que pudieran existir. En algunos casos y dependiendo de la funcionalidad requerida del servidor, podría ser necesario modificar la configuración, que aquí se plantea, para permitir que el equipo proporcione servicios adicionales.

No obstante, se tiene en consideración que los ámbitos de aplicación son muy variados y por lo tanto dependerán de su aplicación, las peculiaridades y funcionalidades de los servicios prestados por las diferentes organizaciones. Por lo tanto, las plantillas y normas de seguridad se han generado definiendo unas pautas generales de seguridad que permitan el cumplimiento de los mínimos establecidos en el ENS y las condiciones de seguridad necesarias en un entorno clasificado.

En el caso de la aplicación de seguridad sobre un entorno perteneciente a una red clasificada, se establece la máxima seguridad posible teniendo en consideración la guía CCN-STIC-301 – Requisitos STIC. Si su sistema requiere de otra configuración menos restrictiva, y está autorizado para ello, consulte el apartado "APLICACIÓN DE NIVELES DE CLASIFICACIÓN" del "ANEXO B" de la guía codificada como CCN-STIC-570A para realizar los pasos adecuados.

Esta guía asume que Exchange Server 2016 va a ser implementado sobre un equipo con Windows Server 2016 Standard de 64 Bits donde se ha seguido el proceso de implantación de seguridad definido en el documento codificado como "CCN-STIC-570A".

Cumpliendo con estos requisitos previos, puede iniciar la instalación de Exchange Server 2016 basado en Microsoft Windows Server 2016 Standard.

Así mismo, no se contempla en esta guía mecanismos de alta disponibilidad o balanceo de carga.

4. ALCANCE

La guía se ha elaborado para proporcionar información específica para realizar una implementación de la solución de MS Exchange Server 2016 Standard o Enterprise en una configuración restrictiva de seguridad. Se incluyen, además, operaciones básicas de administración como la gestión de las bases de datos de buzones, buzones de los usuarios, grupos de distribución, contactos, dominios aceptados y servicios de acceso de clientes entre otros aspectos y aquellas acciones que deben ser llevadas a cabo para el adecuado mantenimiento de la solución.

El escenario en el cual está basada la presente guía tiene las siguientes características técnicas:

a) Un único bosque de Directorio Activo.

b) Un único dominio dentro del bosque de Directorio Activo.

c) Nivel funcional del bosque y del dominio en Windows Server 2016.

d) Un controlador de dominio basado en Windows Server 2016 Standard.

e) Un servidor miembro del dominio basado en Windows Server 2016 Standard.

f) La instalación de Exchange se realiza en modo limpio, es decir no se contemplan procedimientos de migración desde versiones anteriores.

g) En el servidor miembro se instala el rol de servidor de buzones (Mailbox) de Exchange Server 2016.

h) No se contemplan mecanismos de alta disponibilidad ni balanceo de carga en el escenario planteado.

Este documento incluye:

a) **Descripción de las nuevas funcionalidades**, para todos aquellos operadores que tengan experiencia en administrar versiones anteriores a Exchange Server 2016.

b) **Mecanismos para la implementación de la solución.** Se incorporan mecanismos para la implementación de la solución de forma automatizada.

c) **Mecanismos para la aplicación de configuraciones.** Se incorporan mecanismos para la implementación de forma automática de las configuraciones de seguridad susceptibles de ello.

d) **Descripción de la seguridad en Exchange Server 2016.** Completa descripción de los mecanismos de seguridad, autenticación y autorización utilizados en Exchange Server 2016, así como novedades y las medidas adecuadas para reforzar dicha seguridad.

e) **Guía paso a paso.** Permite implementar y establecer las configuraciones de seguridad necesarias en una arquitectura de un servidor Exchange Server 2016.

f) **Lista de comprobación.** Ayuda a verificar el grado de cumplimiento de un servidor con respecto a las condiciones de seguridad que se establecen en esta guía.

g) **Guía de administración.** Proporciona el método para realizar las tareas de administración más comunes en el entorno de seguridad establecido.

5. DESCRIPCIÓN DEL USO DE ESTA GUÍA

Para entender esta guía de seguridad es conveniente explicar el proceso de refuerzo de la seguridad que describe y los recursos que proporciona. Este procedimiento constará de los siguientes pasos:

a) Antes de comenzar a aplicar esta guía, debe tenerse en cuenta que, además de los requisitos a cumplir para la instalación de Exchange Server 2016, será necesario cumplir los requisitos definidos para MS Windows Server 2016, además de ser necesario comprobar los requisitos de otros servicios y aplicaciones que se vayan a aplicar posteriormente como e Internet Information Services 10. En la mayoría de los productos y/o servicios se recomienda tener en particiones distintas para el sistema operativo y el resto de ficheros del servicio proporcionado.

b) Si el entorno que el que está aplicando seguridad pertenece a una red clasificada, se deberá realizar la aplicación de seguridad del sistema operativo y el rol Internet Information Services 10 antes de instalar Exchange Server 2016. Para ello será necesario aplicar las guías de seguridad codificadas como CCN-STIC-570A y CCN-STIC-574. A continuación, se deberá instalar y configurar Exchange Server 2016 sobre Windows Server 2016 tal y como se describe en la presente guía.

c) Al aplicar los procedimientos que se indican en esta guía, deberá tenerse en cuenta que, el servidor deberá contar con al menos dos particiones o volúmenes diferentes: uno para el sistema operativo y otro para la instalación y el almacenamiento de las bases de datos de Microsoft Exchange Server 2016.

d) En aquellos sistemas que les sea de aplicación el ENS estas medidas deberán adaptarse a las necesidades de cada organización.

e) El procedimiento establecido en este documento asume que se está configurando un sistema a partir de un entorno limpio (formateado), en el caso de una red clasificada y un entorno ya en producción, en el caso del ENS.

5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

Los contenidos de esta guía son de aplicación a equipos tipo puesto servidor con Sistema Operativo Windows Server 2016, en castellano, con el objetivo de reducir la superficie de exposición a ataques posibles con una instalación por defecto, manteniendo los principios de máxima seguridad, mínima exposición y servicios y mínimos privilegios que emanan de la CCN-STIC-301. En el caso de llevar a cabo la aplicación de esta guía sobre el Sistema Operativo con una configuración de idioma diferente al castellano, es posible que deba incorporar nuevos recursos y/o realizar ciertas modificaciones sobre los recursos que se adjuntan con este documento para permitir la correcta aplicación y uso del documento.

La guía ha sido probada y verificada con la versión de Exchange Server 2016 sobre el sistema operativo Windows Server 2016 Standard aplicando la guía CCN-STIC-570A para la configuración del Sistema operativo y la guía CCN-STIC-574 para la configuración del rol Internet Information Services 10. No se ha verificado en otros tipos de instalaciones como pudiera ser Windows Server 2016 Datacenter. No obstante, y teniendo en consideración las funcionalidades de ambas versiones de sistema operativo servidor podría llegar a implementarse la siguiente guía sobre la versión Datacenter.

Esta guía se ha diseñado para reducir la superficie de exposición de los equipos servidores que cuenten con una implementación de Exchange Server 2016 en un entorno de dominio de Active Directory.

La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma de virtualización tipo Hyper-V de Windows Server 2012 R2 con las siguientes características técnicas:

a) Servidor Dell PowerEdge™ T320:

   i. Intel Pentium Xeon CPU ES 2430 2.20 GHz.

   ii. HDD 1 TB.

   iii. 64 GB de RAM.

   iv. Interfaz de Red 1 GB.

Esta guía de seguridad no funcionará con hardware que no cumpla con los requisitos de seguridad mínimos de Windows Server 2016. Esto quiere decir que se requieren equipos con procesadores Intel o AMD de 64 bits (x64), con más de 2 GB de memoria RAM.

Así mismo, hay que tener en cuenta que Microsoft Exchange Server 2016 requiere, para una instalación mínima, al menos 8 GB de memora RAM para los servidores de buzones (rol unificado disponible en Exchange Server 2016), aunque se recomienda 16 GB de memoria RAM en entornos en producción.

Esta guía ha sido desarrollada con el objetivo de dotar a la infraestructura de los máximos niveles de seguridad. Es por ello que, es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y por lo tanto pueda ser necesario aplicar acciones adicionales para habilitar servicios o características deseadas tanto en MS Exchange Server 2016 como en MS Windows Server 2016.

Para garantizar la seguridad de los servidores, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio de Microsoft Update. Las actualizaciones, por lo general, se liberan los segundos martes de cada mes, no obstante, hay que tener presente que determinadas actualizaciones por su criticidad pueden ser liberadas en cualquier momento. Se deberá tener en cuenta la implementación de las actualizaciones tanto para el sistema operativo como para los diferentes servicios instalados, como Internet Information Services 10, .NET Framework 4.7.1 (según actualizaciones), y el propio MS Exchange Server 2016, el cual en esta guía se instala con la última actualización acumulativa disponible ya incorporada.

Dependiendo de la naturaleza de estas actualizaciones, el lector podrá encontrarse con algunas diferencias respecto a lo descrito en esta guía. Esto viene motivado por los cambios que en ocasiones se realizan para las distintas actualizaciones de seguridad.

Antes de aplicar esta guía en producción, deberá asegurarse de haber probado el proceso de instalación en un entorno aislado y controlado donde se han aplicado los test y los cambios en la configuración para que se ajusten a los criterios específicos de cada organización.

El espíritu de estas guías no está dirigido a remplazar políticas consolidadas y probadas de las organizaciones, sino servir como la línea base de seguridad que deberá ser adaptada a las necesidades propias de cada organización.

5.2 ESTRUCTURA DE LA GUÍA

Esta guía dispone de una estructura que diferencia la implementación del sistema Microsoft Windows Server 2016 dependiendo del entorno sobre el que vaya a ser aplicado.

La guía dispone de las siguientes configuraciones divididas en dos grandes anexos, los cuales se definen a continuación:

a) **Anexo A:** En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows Server 2016 en su versión Standard con el producto Exchange Server 2016, a las necesidades requeridas por el Esquema Nacional de Seguridad (ENS).

b) **Anexo B:** En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows Server 2016 en su versión Standard con el producto Exchange Server 2016, a las necesidades requeridas en los entornos clasificados.

Cabe remarcar que, en sus respectivos anexos, se dotará de la información necesaria y concreta para cada tipo de implementación.

De manera adicional, en cada una de las carpetas "Scripts" que se adjuntan a los documentos, existe un directorio que almacena un informe en formato HTML con cada objeto de directiva de grupo (GPO) o directiva de grupo local (GPL) que se aplica durante el paso a paso de la guía.

6. SEGURIDAD EN EXCHANGE SERVER 2016

Microsoft Exchange Server 2016 continua su evolución como producto líder en el mercado dentro de las soluciones de comunicación y colaboración. Está basado en las mejoras ya consolidadas de versiones anteriores como la replicación de bases de datos, las directivas de control del trasporte o la administración basada en roles (RBAC).

Es importante recordar que, al igual que en versiones anteriores, los servicios y componentes que forman parte de Exchange Server 2016 están estrechamente integrados en Directorio Activo y dependen de servicios de infraestructura como Internet Information Services (IIS). Es por ello que, es sumamente importante planificar adecuadamente la seguridad de todos estos componentes y aplicar las guías de seguridad CCN-STIC-570A y CCN-STIC-574, en las cuales se establecen las bases de seguridad a nivel de sistema operativo e Internet Information Services, respectivamente, y que posteriormente también va a utilizar Microsoft Exchange Server 2016.

Uno de los principales cambios que ha sufrido Exchange Server 2016, con respecto a versiones anteriores es la reducción del número de roles disponibles desde la instalación. Exchange Server 2016 únicamente presenta un rol de servidor instalable: rol de servidor de buzones (Mailbox). Otros roles como el acceso de clientes, transporte de concentrador o la mensajería unificada se han incorporado como servicios en el rol de servidor de buzones.

Es por ello que, en esta guía, solo se contempla la instalación de un único servidor Exchange Server 2016. En este sentido, cabe señalar que, el servidor de buzones de Exchange Server 2016, incluye todos los componentes de servidor habituales en versiones anteriores: los protocolos de acceso de clientes, el servicio de transporte, las bases de datos de buzones y la mensajería unificada. Así mismo, el servidor de buzones administra la actividad de los buzones activos de ese servidor.

El único rol que mantiene su topología similar a versiones anteriores es el rol de transporte perimetral (**no se contempla su instalación en esta guía**), el cual se implementa normalmente en una red perimetral, fuera del bosque de Directorio Activo interno. Este rol está diseñado para minimizar la superficie expuesta a ataques de la implementación de Exchange. Al controlar todo el flujo del correo accesible desde Internet, también se agregan capas adicionales de protección de mensajes y seguridad contra los virus y el correo no deseado, y se pueden aplicar reglas de flujo del correo (también conocidas como reglas de transporte) para controlar el flujo de mensajes.

Por otro lado, el servicio Outlook en la Web (anteriormente Outlook Web App), ha sido actualizado y optimizado para su uso con tabletas y teléfonos inteligentes, además de diferentes tipos de navegadores.

Tal y como sucede en versiones anteriores, en Microsoft Exchange Server 2016, el flujo de correo se produce a través de la canalización de transporte, la cual es un conjunto de servicios, conexiones, componentes y colas que funcionan al unísono para encaminar todos los mensajes a un categorizador situado en el servicio de transporte en un servidor de buzones de correo dentro de la organización.

La canalización de transporte consta de los siguientes archivos:

a) **Servicio de transporte front-end en servidores de buzones.** Este servicio funciona como un proxy sin estado para todo el tráfico SMTP externo entrante y saliente (opcionalmente) para la organización de Exchange 2016. El servicio de transporte front-end no inspecciona el contenido de los mensajes, no se comunica con el servicio de transporte de buzones en los servidores de buzones de correo ni pone en la cola a ningún mensaje localmente.

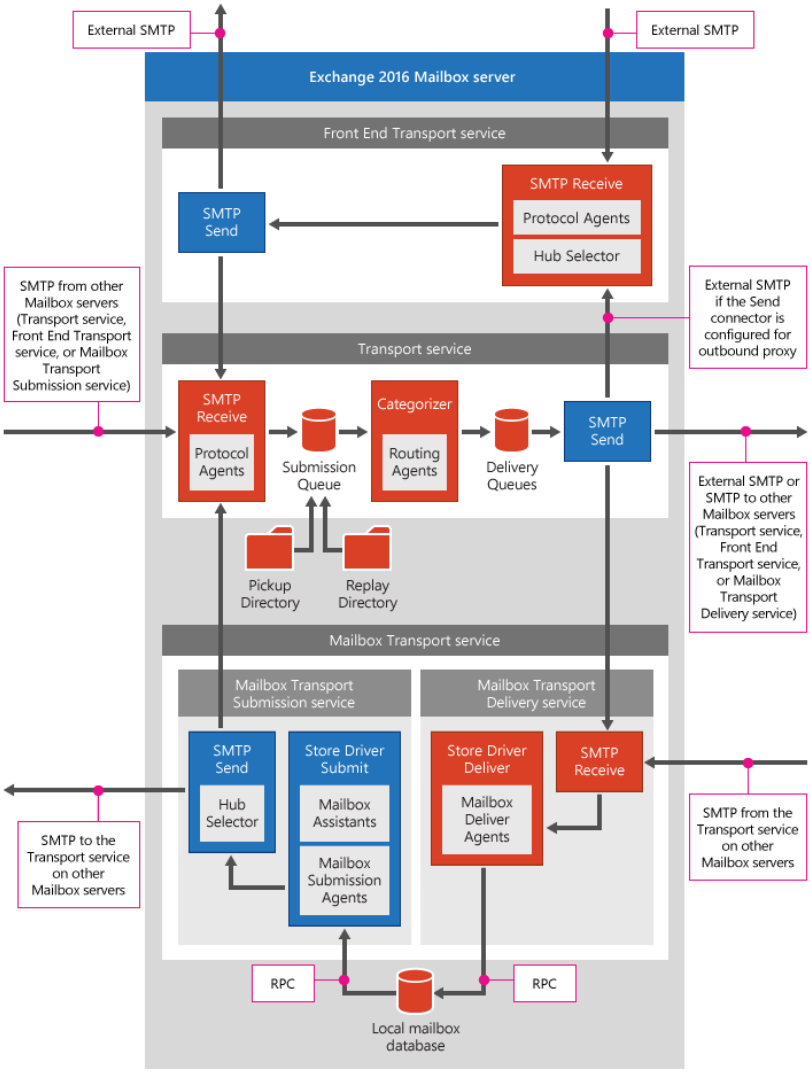
b) **Servicio de transporte en los servidores de buzones de correo.** Este servicio es prácticamente idéntico al servidor de transporte de concentradores en Exchange Server 2013. El servicio de transporte administra todo el flujo de mensajes de SMTP para la organización, categoriza los mensajes e inspecciona el contenido de estos. A diferencia de las versiones anteriores de Exchange, el servicio de transporte nunca se comunica directamente con las bases de datos de los buzones de correo. La tarea, ahora, es administrada por el servicio de transporte de buzón. El servicio de transporte encamina mensajes entre el servicio de transporte de buzones de correo, el servicio de transporte, el servicio de transporte front-end y (según la configuración) el servicio de transporte en los servidores de transporte perimetral.

c) **Servicio de transporte de buzones en los servidores de buzones de correo.** Este servicio consta de dos servicios independientes: el servicio de transporte de envío de buzón de correo y el servicio de entrega de transporte de buzón de correo. El servicio de entrega de transporte de buzón de correo recibe mensajes de SMTP desde el servicio de transporte en el servidor de buzones de correo local o en otros servidores de buzones de correo, y se conecta con la base de datos del buzón de correo usando una llamada a procedimiento remoto (RPC) de Exchange para enviar el mensaje. El servicio de envío de transporte de buzones conecta la base de datos de buzones de correo local con RPC para recuperar mensajes y envía los mensajes por SMTP al servicio de transporte en el servidor de buzones de correo local o en otros servidores de buzones de correo. El servicio de envío de transporte de buzones tiene acceso a la misma información de topología de enrutamiento que el servicio de transporte. Como el servicio de transporte front-end, el servicio de transporte de buzones de correo tampoco coloca en cola a los mensajes localmente.

d) **Servicio de transporte en los servidores de transporte perimetral.** Este servicio es muy similar al servicio de transporte en los servidores de buzones de correo. Si se dispone de un servidor Transporte perimetral instalado en la red perimetral, el flujo de todo el correo procedente de Internet o que se dirige a Internet se producirá a través del servidor Transporte perimetral del servicio de transporte.

Para una mejor comprensión de las interrelaciones entre los diferentes componentes de la canalización del transporte, a continuación, se muestra la arquitectura de cada uno de estos componentes en Exchange Server 2016. Esta información ha sido extraída de Microsoft Docs en la siguiente dirección Web:

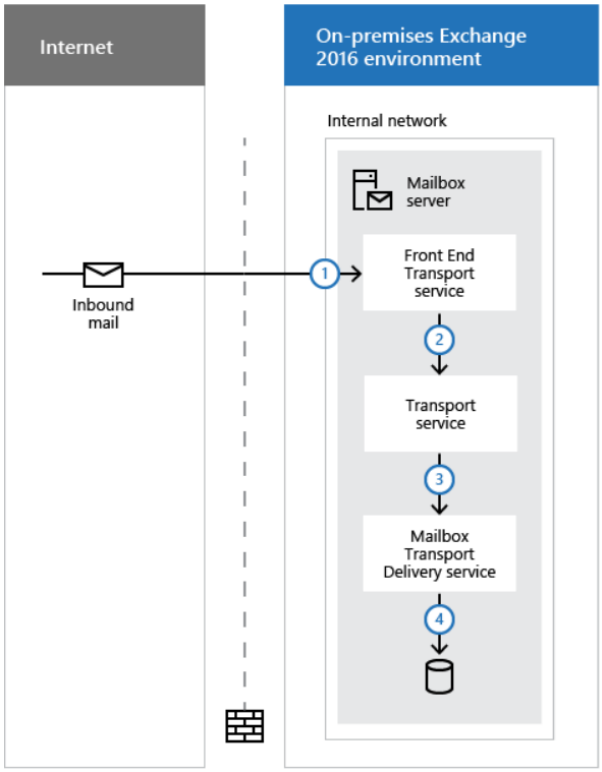
https://docs.microsoft.com/es-es/exchange/mail-flow/mail-flow?view=exchserver-2016



Información general de la canalización de transporte en Exchange Server

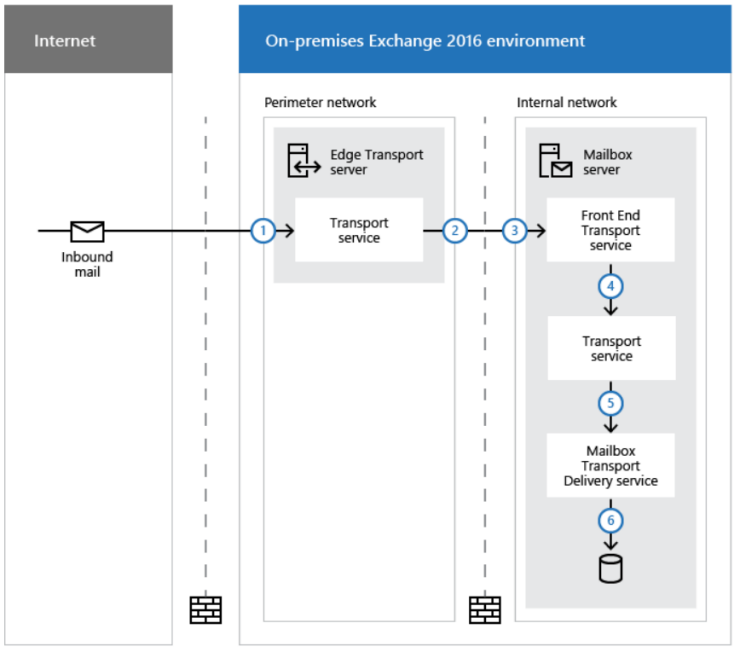
La manera en que los mensajes externos a la organización de Exchange entran en la canalización de transporte, depende de si se dispone de un servidor de transporte perimetral suscrito implementado en la red perimetral u otro servidor independiente que realice las funciones de MTA.

En la siguiente imagen se muestra el flujo de correo entrante cuando no existe ningún servidor de transporte perimetral:



Flujo de correo entrante con sólo los servidores de buzones de Exchange.

En la siguiente imagen se muestra el flujo de correo entrante cuando existe al menos un servidor de transporte perimetral:



Flujo de correo entrante con un servidor de transporte perimetral instalado en la red perimetral.

Los mensajes SMTP internos de la organización entran a la canalización de transporte a través del servicio de transporte en un servidor de buzones de correo de una de las siguientes maneras:

a) Mediante un conector de recepción.

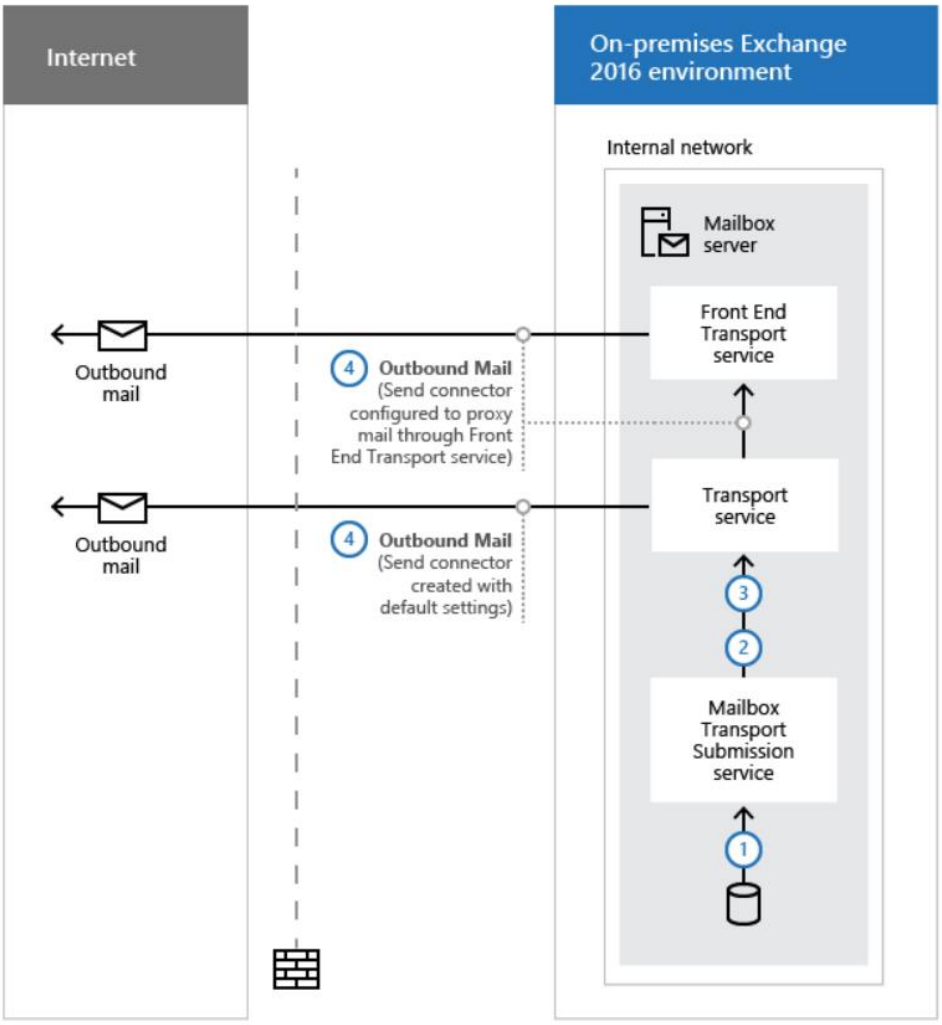
b) Desde el directorio de recogida o reproducción.

c) Desde el servicio de envío de transporte de buzones.

d) Mediante el agente de envío.

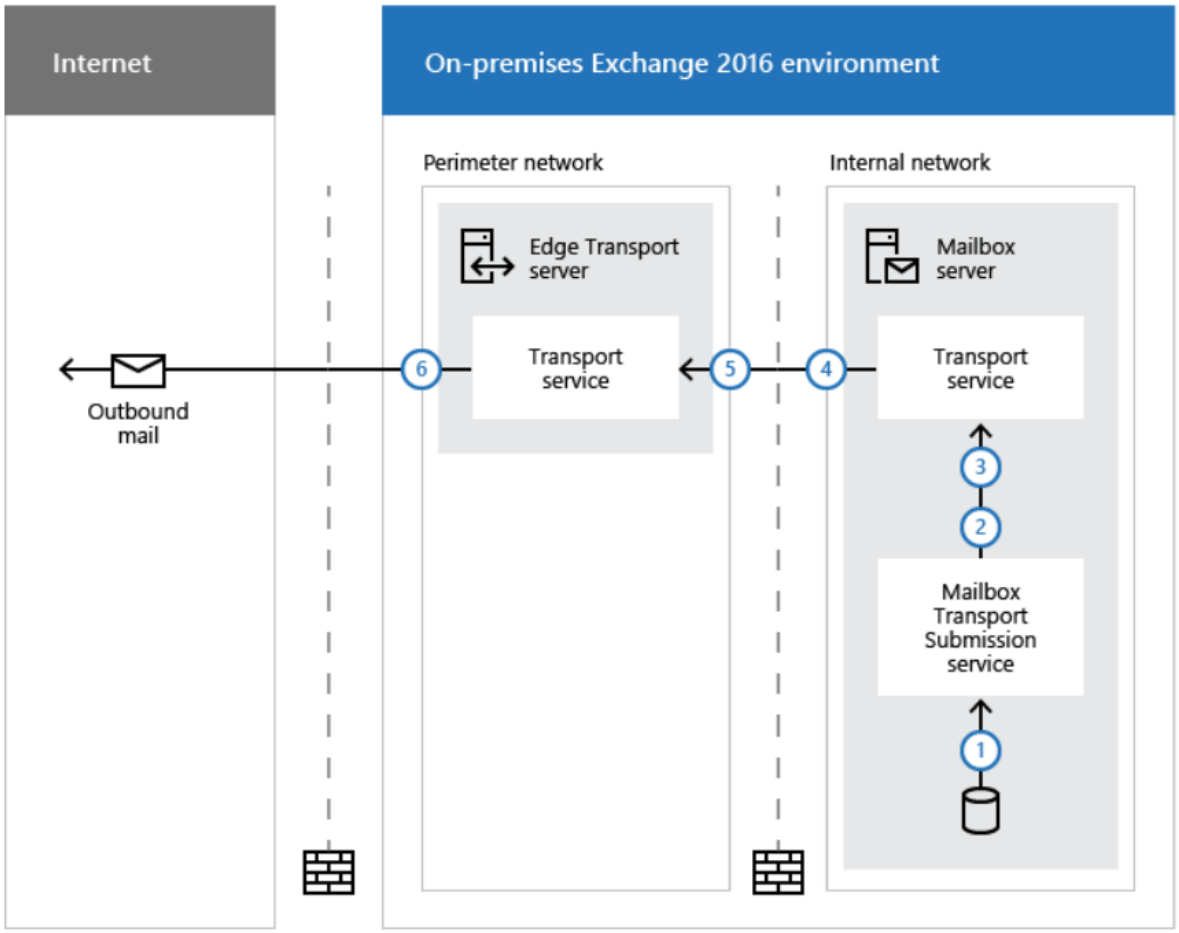
Posteriormente, el mensaje se encamina según el destino de enrutamiento o grupo de distribución.

De forma predeterminada, en una nueva organización de Exchange Server, no existe ningún conector de envío configurado para enviar mensajes a Internet. Se debe crear, al menos un conector de envío para la salida hacia Internet (si procede). Después de hacer esto, el flujo de correo saliente se produce tal como se muestra en la siguiente imagen:



Flujo de mensajes saliente hacia Internet sin un servidor de transporte perimetral

Si se dispone de un servidor de transporte perimetral instalado en la red perimetral, el correo saliente nunca fluye a través del servicio de transporte de front-end. En la siguiente imagen se describe el flujo de correo saliente con un servidor de transporte perimetral.



Flujo de mensajes saliente hacia Internet con un servidor de transporte perimetral

Todos los mensajes que se envían o reciben en una organización de Exchange Server deben clasificarse en el servicio de transporte en un servidor de buzones, antes de que se puedan encaminar y entregar. Después de que se ha clasificado un mensaje, éste se coloca en una cola de entrega para la entrega a la base de datos de buzón de correo de destino, el grupo de disponibilidad de base de datos de destino (DAG), el sitio de Active Directory o bosque de Active Directory, o en el dominio de destino fuera de la organización.

El servicio de transporte en el servidor de buzones de correo está compuesto por los siguientes componentes y procesos:

a) **Recepción de SMTP:** cuando se reciben mensajes por el servicio de transporte, se realiza la inspección de contenido de mensaje, se aplican las reglas de transporte y las de antispam y antimalware si están habilitadas. La sesión SMTP tiene una serie de eventos que funcionan conjuntamente en un orden específico para validar el contenido de un mensaje antes de ser aceptada. Después de que un mensaje haya pasado por completo a través de la recepción SMTP y no ha sido rechazado por un agente antispam o antimalware, se pone en la cola de envío.

b) **Envío (submission):** el envío es el proceso de poner los mensajes en la cola de envío para que el categorizador pueda categorizar dichos mensajes. El envío puede suceder de tres maneras diferentes:

   i. Desde la recepción SMTP, a través de un conector de recepción.

   ii. A través del directorio de recogida o reproducción. Estos directorios existen en servidores de buzones de correo y en los servidores de transporte perimetral. Los archivos de mensaje con formato correcto que se copian en el directorio "Pickup" o en el directorio "Replay" se ponen directamente en la cola de envío.

   iii. A través de un agente de transporte.

c) **Categorizador:** el categorizador coge un mensaje de la cola de envío de uno en uno y lleva a cabo los siguientes pasos:

   i. Resolución del destinatario, que incluye direccionamiento de nivel superior, expansión del grupo de distribución y una bifurcación de mensajes.

   ii. Resolución de encaminamiento.

   iii. Conversión de contenido.

   iv. Además, se pueden aplicar reglas de flujo de correo electrónico definidas por la organización. Después de haber categorizado los mensajes, estos se colocan en la cola de entrega según el destino del mensaje. La base de datos del buzón de destino, DAG, el sitio de Directorio Activo, el bosque de Directorio Activo o el dominio externo colocan los mensajes en la cola.

d) **Envío SMTP:** cómo se entreguen los mensajes desde el servicio de transporte, depende de la ubicación de los destinatarios del mensaje en relación con el servidor de buzones donde se produjo la categorización. El mensaje puede ser entregado a una de las siguientes ubicaciones:

   i. Al servicio de entrega de transporte de buzones en el mismo servidor de buzones de correo.

   ii. Al servicio de entrega de transporte de buzones en otro servidor de buzones de correo que forme parte del mismo DAG.

   iii. Al servicio de transporte en un servidor de buzones de correo en otro DAG, sitio de Directorio Activo o bosque de Directorio Activo.

   iv. Para su entrega en Internet mediante:

   v. Un conector de envío en el mismo servidor de buzón.

   vi. El servicio de transporte en un servidor de buzones diferente.

   vii. El servicio de transporte de front-end en el mismo servidor de buzón o en un servidor de buzón diferente (si el proxy de salida está configurado).

   viii. El servicio de transporte en un servidor de transporte perimetral de la red perimetral.

Es importante conocer los detalles de la canalización de los mensajes para poder diseñar y configurar adecuadamente una topología de Exchange Server 2016, con las medidas de seguridad necesarias en cada escenario.

Por otro lado, los servicios de acceso de clientes en los servidores de buzones proporcionan servicios de autenticación y proxy para las conexiones de clientes internos y externos. Es importante destacar que los servicios de acceso de clientes como tal no realizan ninguna representación de datos, por lo tanto, es un servicio considerado sin estado donde nunca se encuentra nada en cola ni almacenado.

En Exchange Server 2016, los servicios de acceso de cliente forman parte del servidor de buzón de correo, por lo que no se puede instalar un servidor de acceso de cliente independiente como sucedía en versiones anteriores de Exchange.

Aun así, sí que sería posible simular una topología de tipo Front-End, Back-End, similar a la de Exchange Server 2013, si se instalase un servidor de buzones sin integrarlo en un DAG, se moviesen o eliminasen sus bases de datos predeterminadas y, a continuación, se configurase el balanceador de carga o firewall para que las peticiones de clientes solo se dirijan hacia ese servidor. Aunque técnicamente el servidor seguiría siendo un servidor de buzones, desde el punto de vista funcional, actuaría como un servidor de acceso de clientes, al no disponer de bases de datos y actuar de proxy de solicitudes HTTP.

Todos estos cambios en la arquitectura han hecho que se modifique también la forma en que se conectan los clientes Outlook a los servidores Exchange, mejorando también el control sobre las comunicaciones y la seguridad en la conexión.

Uno de los cambios más significativos en este sentido es que el protocolo 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 servicio de acceso de cliente mediante RPC sobre HTTP (también conocido como Outlook Anywhere) y, por lo tanto, este servicio debe estar correctamente configurado, incluyendo los certificados utilizados para la canalización TLS. De no ser así, los clientes de correo como Microsoft Outlook 2010 no podrían conectarse con el servidor Exchange Server 2016. Microsoft Outlook 2007 ya no es compatible con Exchange Server 2016.

Por otro lado, el beneficio de este cambio es que ya no hay necesidad de tener el servicio de acceso de clientes de RPC en el servidor de buzones. Esto ocasiona la reducción de dos espacios de nombres que habitualmente se necesitaban 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.

A partir de Exchange Server 2013 con Service Pack 1, se ha incorporado un nuevo protocolo de comunicación con los clientes Outlook denominado MAPI sobre HTTP (no confundir con RPC sobre HTTP o Outlook Anywhere). Ahora, este protocolo está instalado y habilitado de forma predeterminada en Exchange Server 2016.

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 la federación de identidades, la autenticación de doble factor u otros similares.

MAPI sobre HTTP traslada la capa de transporte al modelo HTTP para mejorar la confiabilidad y la estabilidad de las conexiones de Outlook y de 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. Sin embargo, no todas las versiones de clientes y de servidores son compatibles con MAPI sobre HTTP. A continuación, se muestra una tabla de compatibilidad, incluyendo versiones anteriores de Exchange y Outlook.

Producto	Exchange Server 2016	Exchange Server 2013 SP1	Exchange Server 2013 RTM	Exchange Server 2010 SP3
Outlook 2016	MAPI sobre HTTP Outlook en cualquier lugar	MAPI sobre HTTP Outlook en cualquier lugar	Outlook en cualquier lugar	RPC Outlook en cualquier lugar
Outlook 2013 SP1	MAPI sobre HTTP Outlook en cualquier lugar	MAPI sobre HTTP Outlook en cualquier lugar	Outlook en cualquier lugar	RPC Outlook en cualquier lugar
Outlook 2010 SP2 con las actualizaciones KB2956191 y KB2965295 (14 de abril de 2015)	MAPI sobre HTTP Outlook en cualquier lugar	MAPI sobre HTTP Outlook en cualquier lugar	Outlook en cualquier lugar	RPC Outlook en cualquier lugar
Outlook 2013 RTM	Outlook en cualquier lugar	Outlook en cualquier lugar	Outlook en cualquier lugar	RPC Outlook en cualquier lugar

Outlook 2016 requiere que el servicio autodiscover esté configurado y funcionando correctamente o, de lo contrario, no se podrá conectar a Exchange Server. Outlook 2016 recibe las configuraciones de conexión directamente desde el servicio Autodiscover, en vez del registro de Windows, haciendo que los perfiles de usuarios estén actualizados en todo momento, pero también haciendo que el servicio autodiscover sea una característica requerida.

En Exchange Server 2016, Outlook emplea el servicio autodiscover para crear un nuevo punto de conexión compuesto por el identificador único del buzón (mailbox GUID), el símbolo @ y la parte de dominio de la dirección SMTP principal del usuario. Este sencillo cambio da como resultado la práctica eliminación del mensaje "Su administrador ha realizado un cambio en su buzón de correo. Reinicie".

Desde el punto de vista de la seguridad, las directrices de refuerzo de la seguridad seguidas y aplicadas en anteriores versiones de Exchange Server siguen siendo válidas para Exchange Server 2016, las cuales se pueden resumir en los principales aspectos:

a) Aplicar un modelo de seguridad en profundidad donde se incluyan todos los elementos que intervienen en el servicio como son componentes de red, sistemas operativos, servicios y aplicaciones.

b) Habilitar únicamente los servicios necesarios para la comunicación de los usuarios. Se recomienda especialmente deshabilitar protocolos inseguros como POP3 o IMAP4.

c) Cifrar comunicaciones internas y externas de cualquier naturaleza y protocolo.

d) Habilitar la característica nativa de Exchange Server denominada seguridad de dominio (Mutual TLS) en todos aquellos dominios y espacios de nombres SMTP cuya comunicación incluya contenido potencialmente sensible.

e) 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.

f) Autenticar siempre usuarios y equipos antes de hacer uso de los servicios de correo electrónico.

g) Configurar mecanismos de defensa ante correo electrónico no deseado y código dañino.

h) Habilitar los registros de auditoría y acceso a los buzones.

i) Configurar directivas de transporte y agentes de conformidad.

j) Utilizar el protocolo Kerberos como mecanismo de autenticación entre servidores y equipos miembros del dominio.

k) Utilizar autenticación basada en formularios para el acceso externo a Outlook en la Web sobre TLS 1.2 y autenticación integrada sobre TLS 1.2 para el resto de servicios de movilidad.

l) Implementar directivas de refuerzo de la seguridad para Exchange Server 2016 en los servidores donde esté instalado el producto.

m) Implementar directivas de seguridad de Firewall.

n) Aplicar todas las actualizaciones disponibles por el fabricante tanto para el propio Exchange como para todos sus componentes y el sistema operativo.

o) Aplicar un control estricto de roles de usuarios que tienen acceso a la consola Web de administración (Exchange Admin Center), auditoría, exhibición de documentos electrónicos (in-place eDiscovery) y buzones en Exchange Server.

p) Instalar y configurar una solución antivirus desarrollada especialmente para Exchange Server 2016 que permita detectar código dañino tanto en el transporte como en elementos almacenados en las bases de datos de buzones.

Además de estas recomendaciones, Exchange Server 2016 incluye las mejoras de seguridad ya incorporadas desde versiones anteriores, y que continúan fortaleciendo la infraestructura de correo electrónico en todos sus ámbitos:

a) Protección frente a código dañino. El servicio de transporte implementado en los servidores de buzones incluye una protección básica frente a código dañino de un único motor. Dicha protección se limita a analizar los mensajes en tránsito, en ningún caso se analizan los mensajes almacenados en las bases de datos. Este servicio requiere acceso a internet o una descarga manual de las actualizaciones de código dañino, las cuales se actualizan cada hora de forma predeterminada. En Exchange 2016, la configuración y administración de los agentes antimalware sólo está disponible en el Shell de administración de Exchange. Se recomienda, en entornos en producción, completar esta protección básica con un servicio antimalware de terceros.

b) Protección frente a correo electrónico no deseado. De forma predeterminada, los agentes contra el correo electrónico no deseado no están habilitados en un servidor de buzones de Exchange Server 2016 y se habilitan, normalmente, si la organización no tiene ningún servidor de transporte perimetral o si no realiza otro tipo de filtrado de correo electrónico no deseado en los mensajes entrantes. Los agentes implementados en el servidor de buzones son: agente de filtro de remitente, agente de ID de remitente, agente de filtro de contenido y agente de análisis de protocolo (reputación de remitente).

Nota: Es muy importante tener en cuenta que: desde el 1 de noviembre de 2016, Microsoft ha dejado de desarrollar actualizaciones de definición de correo no deseado para los filtros de SmartScreen de Exchange y Outlook, incluyendo Exchange Server 2016. Las definiciones de spam SmartScreen existentes aún se pueden descargar, pero se reducirá en su eficacia a través del tiempo. Más información en: https://blogs.technet.microsoft.com/exchange/2016/09/01/deprecating-support-for-smartscreen-in-outlook-and-exchange/

c) Acceso deshabilitado a la consola Web de administración de Exchange. Por motivos de seguridad, Exchange Server 2016 permite habilitar o deshabilitar el acceso a la consola de administración (Exchange Admin Center) para aquellos usuarios que se conectan desde Internet.

d) Administración de la carga de trabajo. Cada carga de trabajo de Exchange consume recursos del sistema como CPU, operaciones de la base de datos de buzones de correo o solicitudes de Directorio Activo, para ejecutar solicitudes del usuario o trabajos en segundo plano. Las cargas de trabajo de Exchange Server 2016 se pueden administrar controlando la forma en que los usuarios individuales consumen los recursos, de tal forma que se limitan los daños producidos por el abuso que algunos usuarios pueden hacer de la infraestructura. Aunque ya era posible dicho control en Exchange Server 2010, esta capacidad se ha ampliado para Exchange Server 2013 y 2016.

e) Conservación local y retención por juicio. Cuando existen sospechas fundadas de posibles litigios, se solicita a las organizaciones que conserven toda la información almacenada electrónicamente, incluso el correo electrónico que sea relevante para el caso. Si el correo electrónico no se conserva, la organización puede quedar expuesta a riesgos legales o financieros, como sentencias judiciales adversas, sanciones o multas. En Exchange Server 2016, la conservación local introduce un nuevo modelo que permite especificar los parámetros siguientes:

   i. Qué retener. El auditor o responsable del caso, puede especificar qué elementos desea retener mediante parámetros de consulta como palabras clave, remitentes y destinatarios, fechas de inicio y finalización, así como especificar los tipos de mensajes que desea retener.

   ii. Duración de la retención. Se puede especificar una duración para la retención de elementos.

f) Prevención de pérdida de datos. La característica de prevención de pérdidas de datos permite habilitar directivas en el transporte que inspeccionen el correo y los datos adjuntos en busca de información sensible que se debe proteger o bloquear como números de identificación o números de tarjeta de crédito. Así mismo, Exchange Server 2016 permite crear huellas digitales de documentos, lo cual le ayuda a detectar información confidencial en formularios estándar.

g) Control de acceso basado en roles. Exchange Server 2016 continúa con el modelo de control de acceso basado en roles, incrementando el número de roles predeterminados e integrando su gestión en la consola Web de administración.

h) Escenarios de compartición para usuarios. Exchange Server 2016 admite diversos escenarios de compartición de información entre usuarios de diferentes organizaciones, e incluso servicios de nube como Microsoft Office 365. Las tecnologías involucradas en estos escenarios son la federación, las relaciones de organización y las directivas de uso compartido.

   i. Federación. La federación en Microsoft Exchange Server 2016 permite a los usuarios colaborar con otros usuarios externos compartiendo la información de calendario o de contactos con los destinatarios en otras organizaciones federadas externas. También es posible la colaboración entre bosques sin tener que configurar y administrar relaciones de confianza de Directorio Activo.

ii. Relaciones de organizaciones. Una relación entre organizaciones es una relación de uno a uno que habilita a los usuarios en cada organización ver información de disponibilidad de calendario. Se puede establecer el nivel de información que la organización externa puede visualizar: Sin acceso, acceso de disponibilidad o acceso de disponibilidad, incluyendo tiempo, asunto y ubicación. La creación de una relación de organización representa uno de los pasos de la configuración del uso compartido federado de la organización de Exchange, y requiere configurar una confianza de federación para la organización local de Exchange.

iii. Directivas de uso compartido. Estas directivas permiten a los usuarios designados administrar y compartir su propio calendario con destinatarios externos a la organización. Se puede aplicar tanto a organizaciones federadas como a otras organizaciones a través de la capacidad de publicación de calendarios de Internet que incorpora Microsoft Outlook.

i) Information Rights Management. Exchange 2016 mejora las características de control y protección de la seguridad para proteger el contenido confidencial de los mensajes en varios niveles; asimismo, mantiene la capacidad de la organización de descifrar, buscar y aplicar directivas de mensajería a contenido protegido.

6.1 MÉTODOS RECOMENDADOS PARA INSTALAR Y MANTENER UN ENTORNO DE EXCHANGE SERVER 2016 MÁS SEGURO

A continuación, se mencionan una serie de métodos a tener en cuenta durante el proceso de instalación de Exchange Server 2016 que ayudan a mejorar su seguridad:

a) **Instalación delegada.** El primer servidor de Exchange 2016 que se instala en la organización requiere que la cuenta que se usa para ejecutar el programa de instalación pertenezca al grupo Administradores de empresa. Dicha cuenta se agrega posteriormente al grupo de roles de administración de la organización creado por el programa de instalación de Exchange 2016. La instalación delegada puede usarse para que los administradores que no pertenezcan al grupo de roles de administración de la organización configuren los servidores subsiguientes.

b) **Permisos del sistema de archivos.** El programa de instalación asigna los permisos mínimos necesarios en el sistema de archivos donde se almacenan los datos y archivos binarios de Exchange. No se debe realizar ningún cambio en las listas de control de acceso de las carpetas raíz y archivos de programa del sistema de archivos.

c) **Rutas de instalación.** Se recomienda instalar los archivos binarios de Exchange 2016 en una unidad que no sea del sistema (un volumen en el que no esté instalado el sistema operativo). Las bases de datos y los registros de transacciones de Exchange pueden aumentar de tamaño rápidamente y deben ubicarse en volúmenes no pertenecientes al sistema para que no disminuya la capacidad ni el rendimiento. Otros registros generados por diferentes componentes de Exchange, por ejemplo, los registros de transporte se almacenan también en la misma ruta de instalación que los archivos binarios de Exchange y su tamaño puede aumentar considerablemente según la configuración y el entorno de mensajería.

En Exchange 2016 puede configurarse el tamaño máximo de muchos archivos de registro y el espacio máximo de almacenamiento que puede ocupar una carpeta de archivos de registro, que tiene un valor predeterminado de 250 Megabytes. Para prevenir una posible interrupción del sistema debido a poco espacio en disco, se recomienda que se calculen los requisitos de registro para cada rol del servidor y se configuren las opciones de registro y las ubicaciones de almacenamiento de los archivos de registro en consonancia con ellos.

d) **Bloqueo de clientes heredados de Outlook.** Teniendo en cuenta sus requisitos, el bloqueo de clientes de Outlook se puede configurar para que bloquee las versiones cliente heredadas de Outlook. Algunas características de Exchange 2016, por ejemplo, el protocolo de acceso MAPI HTTP, las reglas de protección de Outlook y los archivos personales, no admiten clientes heredados de Outlook.

e) **Separación de direcciones SMTP y nombres de usuario.** De forma predeterminada, Exchange genera alias y direcciones de correo electrónico a partir del nombre de usuario del buzón de correo. Muchas organizaciones crean una directiva adicional de direcciones de correo electrónico para separar las direcciones de correo electrónico de los usuarios de los nombres de usuarios con el fin de incrementar la seguridad. Asimismo, puede separar las direcciones de correo electrónico de los nombres de usuario especificando un alias diferente del nombre de usuario que se usa al crear o habilitar un buzón de correo.

Así mismo, ya no es necesario instalar ni ejecutar las herramientas siguientes:

a) La herramienta de seguridad URLScan no se necesita en IIS 10. En versiones anteriores de Microsoft Exchange, era habitual instalar herramientas de IIS como URLScan para proteger una instalación de IIS. Exchange 2016 requiere Windows Server 2016, el cual incluye IIS 10, y todas las características de seguridad que originalmente estaban en URLScan están disponibles en el Filtrado de solicitudes de IIS 10.

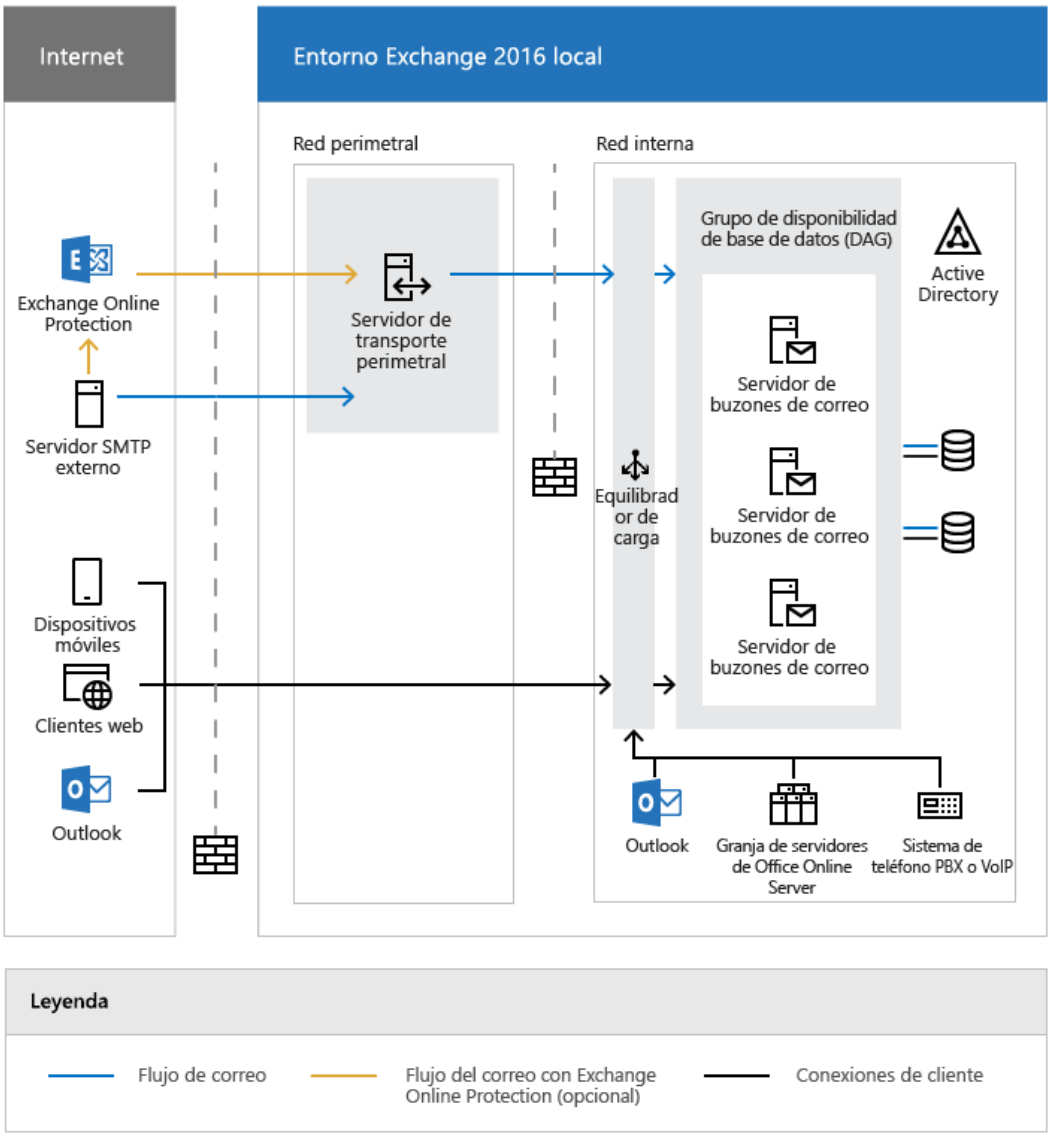
b) Ya no hace falta instalar Exchange Best Practices Analyzer. En versiones anteriores de Microsoft Exchange era habitual instalar Exchange Best Practices Analyzer antes de la instalación y después ejecutarlo periódicamente. El programa de instalación de Exchange 2016 incluye los componentes de Exchange Best Practices Analyzer y los ejecuta durante la instalación. Antes de la instalación no hace falta ejecutar Exchange Best Practices Analyzer.

c) Ya no se necesita el asistente para configuración de seguridad (SCW) ni las plantillas de Exchange para SCW. El programa de instalación de Exchange 2016 instala solamente los servicios necesarios y crea reglas de Firewall de Windows Firewall con Seguridad avanzada para abrir únicamente los puertos necesarios en los servicios y procesos de ese rol del servidor. Exchange 2016 no se incluye con plantillas de SCW.

6.2 RELACIÓN DE PUERTOS, MECANISMOS DE AUTENTICACIÓN Y CIFRADO PARA LAS RUTAS DE DATOS ENTRE SERVIDORES EXCHANGE 2016

Nota: No se admiten configuraciones en las que se incluye un firewall entre servidores de buzones que se encuentran en el mismo sitio de Directorio Activo. Si se dispone de un firewall o dispositivos de red que puedan restringir o modificar este tipo de tráfico de red, se deben configurar las reglas necesarias para que se permita una comunicación libre y sin restricciones entre estos servidores (tráfico de red entrante y saliente en cualquier puerto, incluidos los puertos RPC aleatorios, así como cualquier protocolo que nunca altere los bits en la conexión).

Exchange Server 2016 emplea una única arquitectura de bloques que permite proporcionar servicios de correo electrónico en organizaciones de cualquier tamaño, desde pequeñas empresas a las principales organizaciones multinacionales. Esta arquitectura se describe en la siguiente imagen.



Arquitectura de Exchange Server 2016.

La comunicación entre los servidores Exchange y las versiones anteriores y futuras de Exchange se produce en el nivel de protocolo. No se permite la comunicación entre niveles. Esta arquitectura de comunicación se resume como "cada servidor es una isla" y tiene las siguientes ventajas:

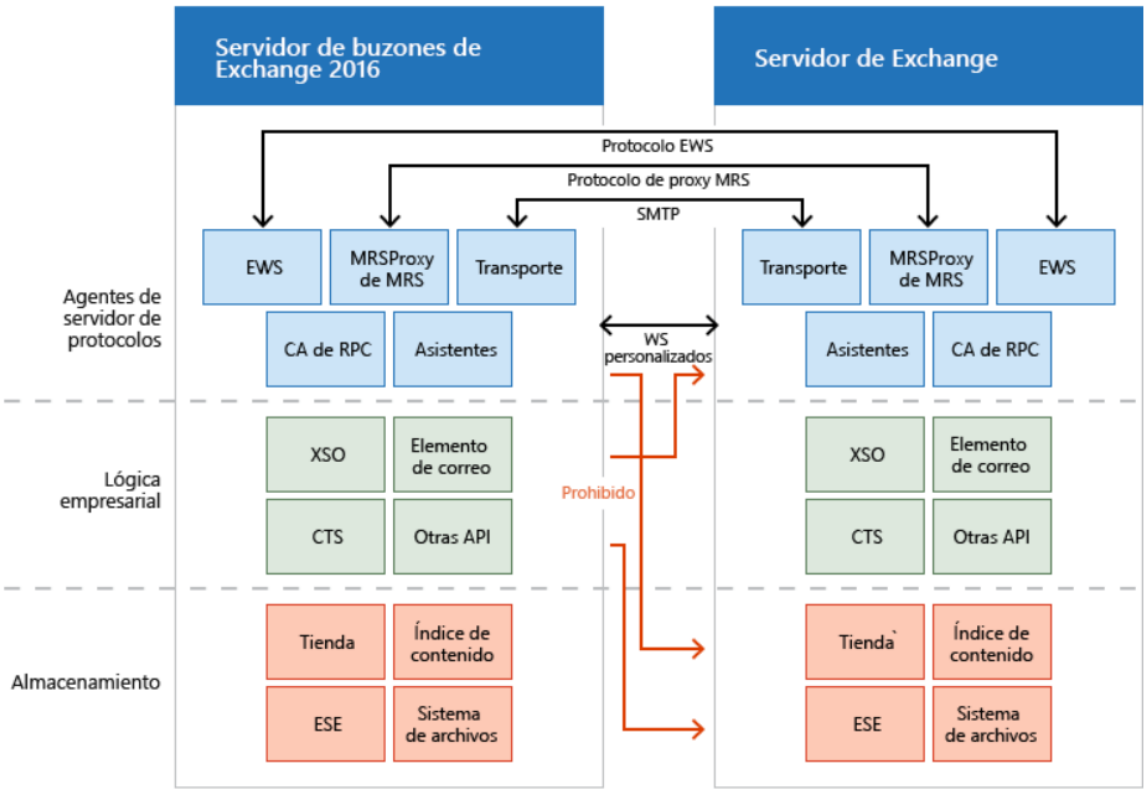
a) Comunicaciones reducidas entre servidores.

b) Comunicaciones con reconocimiento de versión.

c) Errores aislados.

d) Diseño integrado en cada servidor.

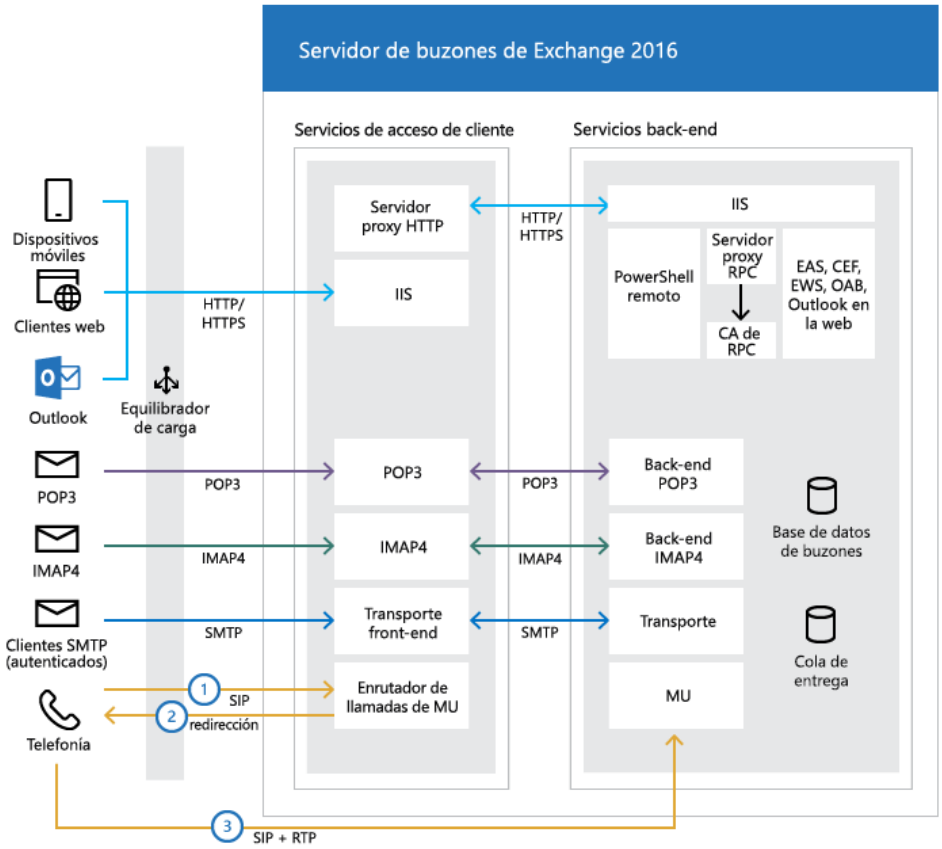
En la siguiente imagen se muestra la comunicación global de nivel de protocolo que se produce entre diferentes servidores de Exchange.



Comunicación de nivel de protocolo entre servidores de Exchange.

Por otro lado, los servicios de acceso de cliente de los servidores de buzones de Exchange Server 2016 son responsables de aceptar cualquier tipo de conexión de cliente. Cuando se reciben peticiones de conexión de los clientes en los servicios front-end, se crean inmediatamente conexiones proxy a los servicios back-end en el servidor de buzones de correo de destino (ya sea el servidor local o un servidor de buzones remoto que contiene la copia activa del buzón del usuario).

Es por ello que, los clientes nunca se conectan directamente a los servicios back-end, tal y como se muestra en la imagen siguiente:



Esquema de comunicaciones de clientes de Exchange.

El protocolo que usa un cliente determina el protocolo usado para canalizar mediante proxy la solicitud a los servicios back-end en el servidor de buzones de correo de destino. Por ejemplo, si el cliente se ha conectado mediante HTTP, el servidor de buzones de correo usa HTTP para canalizar mediante proxy la solicitud al servidor de buzones de correo de destino (protegido mediante TLS con un certificado autofirmado). Si el cliente ha usado IMAP o POP, el protocolo que se usa es IMAP o POP, y así sucesivamente.

La única excepción a esto, son las solicitudes de telefonía, las cuales son diferentes al resto de conexiones de cliente. En lugar de canalizar la solicitud mediante proxy, el servidor de buzones de correo la redirige al servidor de buzones de correo que contiene la copia activa del buzón del usuario. Los dispositivos de telefonía tienen que establecer sus sesiones SIP y RTP directamente con los servicios de mensajería unificada en el servidor de buzones de correo de Exchange 2016 de destino.

Tal y como se ha indicado anteriormente, en Exchange Server 2013 o versiones anteriores, se podía instalar el rol de servidor de acceso de clientes y el rol de servidor de buzones de correo en equipos distintos. Sin embargo, en Exchange 2016, el rol de servidor de acceso de clientes se instala automáticamente como parte del rol de servidor Buzón y ya no está disponible como opción de instalación independiente.

Este cambio refleja la filosofía de ubicación compartida de roles de servidor de Exchange, que es uno de los procedimientos recomendados desde Exchange Server 2010. Una arquitectura de servidor Exchange de varios roles ofrece las siguientes ventajas tangibles:

a) Todos los servidores de la organización Exchange (con la excepción de los servidores de transporte perimetral) pueden ser idénticos: el mismo hardware, la misma configuración y las mismas funciones. Esta uniformidad simplifica la adquisición de hardware y también el mantenimiento y la administración de los servidores de Exchange.

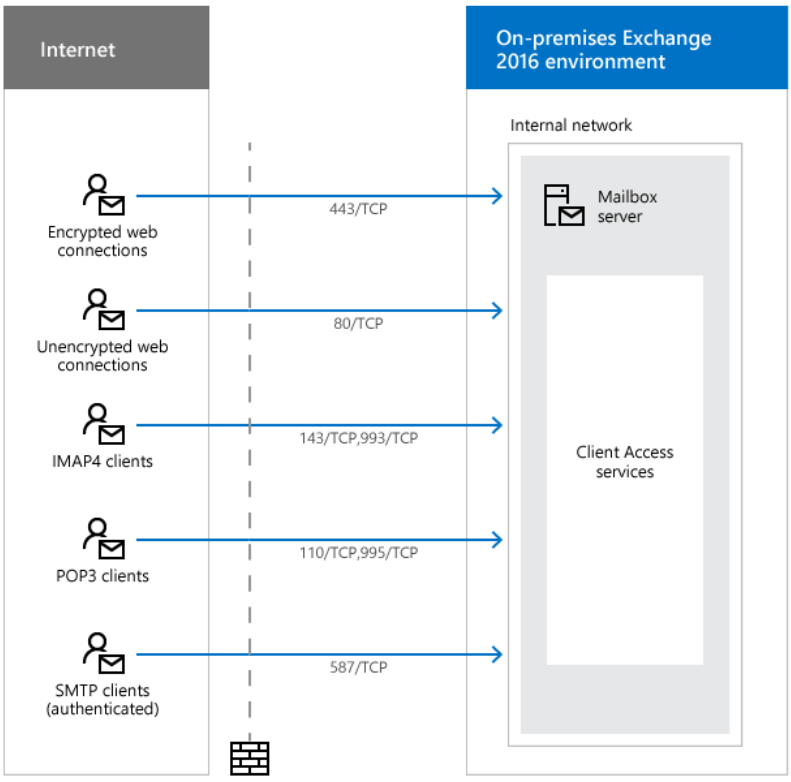
b) Debido a esto, es posible que, en entornos grandes, se requieran menos servidores físicos de Exchange. Esto se traduce en menos costes de mantenimiento continuo, menor número de licencias de servidor Exchange y menos requisitos de espacio físico y alimentación.

c) Se mejora la escalabilidad, ya que se distribuye la carga de trabajo entre un número mayor de máquinas físicas. Durante un error, la carga de los restantes servidores Exchange de varios roles aumenta de forma equilibrada, lo que garantiza que los demás servicios de Exchange no se vean afectados de manera negativa.

d) Se ha mejorado la resistencia a fallos, ya que un servidor Exchange de varios roles puede soportar un mayor número de errores del rol (o servicio) Acceso de cliente y seguir prestando servicio.

A continuación, se ofrece información sobre los puertos de red que usa Microsoft Exchange Server 2016 para la comunicación con clientes de correo electrónico, servidores de correo de Internet y otros servicios externos a la organización de Exchange local. Estos puertos no han variado sustancialmente desde Exchange Server 2013.

Hay que recordar que, en Exchange Server 2016, el acceso de cliente (front-end) y los servicios back-end se instalan en el mismo servidor de buzón de correo.



Puertos de red utilizados para la comunicación de clientes

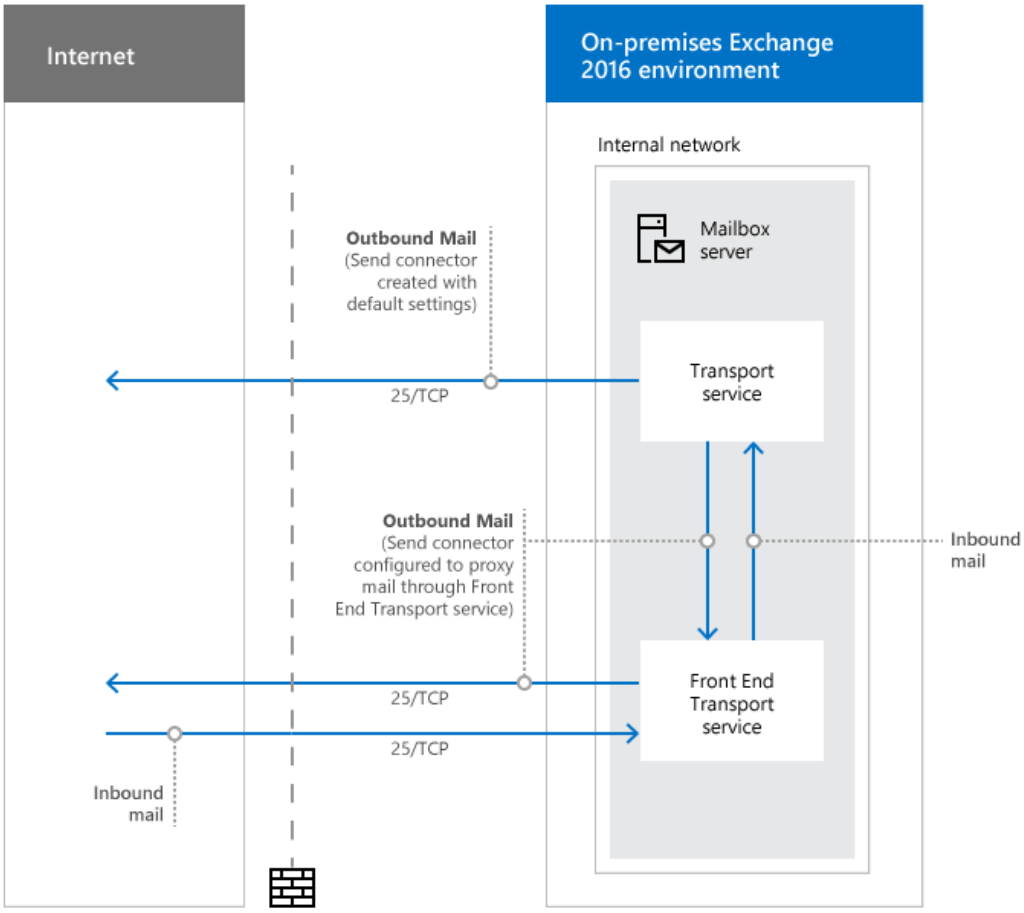
6.2.1 PUERTOS DE RED NECESARIOS PARA CLIENTES Y SERVICIOS

En la siguiente tabla, se muestran los principales puertos y servicios utilizados por clientes y servidores de Exchange Server 2016.

Servicio o finalidad	Puertos	Admite cifrado	Cifrado predeterminado
Servicio de detección automática	443/TCP (HTTPS)	SI	SI
Exchange ActiveSync	443/TCP (HTTPS)	SI	SI
Servicios Web Exchange (EWS)	443/TCP (HTTPS)	SI	SI
Distribución (OAB) de la libreta de direcciones sin conexión	443/TCP (HTTPS)	SI	SI
Outlook Anywhere (RPC sobre HTTP)	443/TCP (HTTPS)	SI	SI
Outlook MAPI a través de HTTP	443/TCP (HTTPS)	SI	SI
Outlook en la web	443/TCP (HTTPS)	SI	SI
Publicación de calendarios de Internet	80/TCP (HTTP)	SI	NO
Outlook en la web (redireccionamiento a 443/TCP)	80/TCP (HTTP)	SI	NO
Detección automática (reserva cuando 443/TCP no está disponible)	80/TCP (HTTP)	SI	NO
IMAP4, clientes	143/TCP (IMAP), 993/TCP (IMAP seguro)	SI	SI
POP3, clientes	110/TCP (POP3), 995/TCP (POP3 seguro)	SI	SI
Clientes SMTP (autenticados)	587/TCP (SMTP autenticado)	SI	SI

6.2.2 PUERTOS DE RED NECESARIOS PARA EL FLUJO DE CORREO

En la imagen y la tabla siguientes se muestran los puertos de red necesarios para el flujo de correo en una organización Exchange Server 2016.



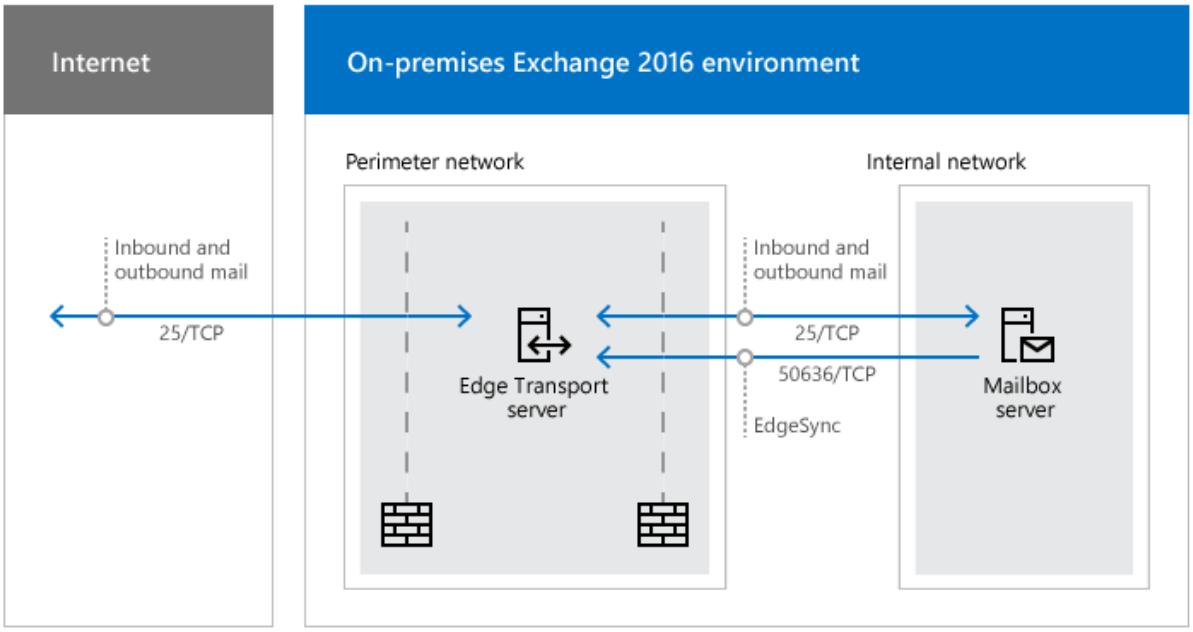
Puertos de red utilizados en el flujo de correo sin un servidor perimetral

Servicio o finalidad	Puertos	Origen	Destino	Admite cifrado	Cifrado predeterminado
Correo entrante	25/TCP (SMTP)	Internet	Servidor de buzones	SI	SI (TLS oportunista)
Correo saliente	25/TCP (SMTP)	Servidor de buzones	Internet	SI	SI (TLS oportunista)
Correo saliente (si se redirige con el servicio de transporte front-end)	25/TCP (SMTP)	Servidor de buzones	Internet	SI	SI (TLS oportunista)
DNS para la resolución de nombres del siguiente salto del correo	53/UDP, 53/TCP (DNS)	Servidor de buzones	Servidor DNS	NO	NO

6.2.3 PUERTOS DE RED NECESARIOS PARA EL FLUJO DE CORREO CON SERVIDORES DE TRANSPORTE PERIMETRAL

Aunque no es objetivo de esta guía la instalación de un servidor perimetral, únicamente con carácter informativo, se muestra la información de puertos necesarios para el flujo de correo cuando existe un servidor de transporte perimetral suscrito e instalado en la red perimetral.

En este escenario, el correo saliente desde la organización de Exchange nunca fluye a través del servicio de transporte Front-End en los servidores de buzones. Por el contrario, el correo fluye siempre desde el servicio de transporte de un servidor de buzones situado en el sitio de Directorio Activo en el cual está suscrito el servidor de transporte perimetral, directamente hacia el servidor perimetral. Esto sucede independientemente de la versión de Exchange en el servidor de transporte perimetral.



Puertos de red utilizados en el flujo de correo con un servidor perimetral

Correo entrante: Internet a servidor de transporte perimetral

Información	Parámetros
Puertos	25/TCP (SMTP)
Origen	Internet
Destino	Servidor de transporte perimetral
Admite cifrado	SI
Cifrado predeterminado	SI (TLS oportunista)

Correo entrante: servidor de transporte perimetral en organización de Exchange interna

Información	Parámetros
Puertos	25/TCP (SMTP)
Origen	Servidor de transporte perimetral
Destino	Servidores de buzones de correo en el sitio suscrito de Active Directory
Admite cifrado	SI
Cifrado predeterminado	SI (TLS oportunista)

Correo saliente: organización de Exchange interna a servidor de transporte perimetral

Información	Parámetros
Puertos	25/TCP (SMTP)
Origen	Servidores de buzones de correo en el sitio suscrito de Active Directory
Destino	Servidor de transporte perimetral
Admite cifrado	SI
Cifrado predeterminado	SI (M-TLS)

Correo saliente: servidor de transporte perimetral a Internet

Información	Parámetros
Puertos	25/TCP (SMTP)
Origen	Servidor de transporte perimetral
Destino	Internet
Admite cifrado	SI
Cifrado predeterminado	SI (TLS oportunista)

Sincronización de EdgeSync

Información	Parámetros
Puertos	50636/TCP (LDAP seguro)
Origen	Servidores de buzones de correo en el sitio suscrito de Active Directory
Destino	Servidor de transporte perimetral
Admite cifrado	SI
Cifrado predeterminado	SI

DNS para la resolución de nombres del siguiente salto del correo (no mostrado)

Información	Parámetros
Puertos	53/UDP - 53/TCP (DNS)
Origen	Servidor de transporte perimetral
Destino	Servidor DNS
Admite cifrado	NO
Cifrado predeterminado	NO

Detección de servidor proxy abierto en la reputación del remitente

Información	Parámetros
Puertos	SOCKS4, SOCKS5: 1081, 1080 - Wingate, Telnet, Cisco: 23 - HTTP CONECT, HTTP POST: 6588, 3128, 80
Origen	Servidor de transporte perimetral
Destino	Internet
Admite cifrado	NO
Cifrado predeterminado	NO

6.2.4 SERVICIOS DE EXCHANGE SERVER 2016

En las siguientes tablas se identifican todos los servicios de Exchange Server 2016 que se registran durante el proceso de instalación:

Topología de Active Directory de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeADTopology
Descripción y dependencias	Proporciona información de topología de Active Directory para los servicios de Exchange. Si este servicio se detiene, no se puede iniciar la mayoría de los servicios de Exchange.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Servicio de uso compartido de puertos Net.TCP
Obligatorio u opcional	Obligatorio

Actualización contra correo no deseado de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeAntispamUpdate
Descripción y dependencias	Proporciona actualizaciones de definición de correo no deseado de Exchange SmartScreen.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Opcional

Auditoría de cumplimiento de normas de Microsoft Exchange

Información	Parámetros
Nombre corto	MSComplianceAudit
Descripción y dependencias	Proporciona características de auditoría de Exchange.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Obligatorio

Servicio de cumplimiento de normas de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeCompliance
Descripción y dependencias	Proporciona un host para servicios de cumplimiento de normas de Exchange.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Obligatorio

Administración de Microsoft Exchange DAG

Información	Parámetros
Nombre corto	MSExchangeDagMgmt
Descripción y dependencias	Proporciona almacenamiento y base de datos de administración de diseño para los servidores de buzones de correo en grupos de disponibilidad de base de datos (dag).
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Servicio de uso compartido Microsoft Exchange Active Directory TopologyNet.TCP puerto
Obligatorio u opcional	Obligatorio

Diagnósticos de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeDiagnostics
Descripción y dependencias	Proporciona a un agente que supervisa el estado del servidor Exchange.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Ninguno
Obligatorio u opcional	Obligatorio

EdgeSync de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeEdgeSync
Descripción y dependencias	Replica datos de destinatarios y de configuración entre el servidor de buzón de correo y los servicios de directorio ligero de Active Directory (AD LDS) en los servidores de transporte perimetral suscritos a través de un canal LDAP seguro. Si no dispone de los servidores de transporte perimetral suscritos, puede deshabilitar este servicio.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Opcional

Transporte de front-end de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeFrontEndTransport
Descripción y dependencias	Conexiones de servidores proxy SMTP de los hosts externos con el servicio de transporte de Microsoft Exchange en los servidores de buzones (el servidor local o servidores remotos).
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Obligatorio

Administrador de mantenimiento de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeHM
Descripción y dependencias	Parte de disponibilidad administrada que supervisa el estado de los componentes clave en el servidor de Exchange.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Instrumental de administración de Windows (evento) LogWindows
Obligatorio u opcional	Obligatorio

Recuperación de administrador de mantenimiento de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeIMAP4
Descripción y dependencias	Conexiones de cliente de IMAP4 los servidores proxy de los servicios de acceso de cliente (frontend) con el servicio back-end IMAP4 en los servidores de buzones. De forma predeterminada, este servicio no se está ejecutando, por lo que los clientes IMAP4 no se pueden conectar al servidor de Exchange hasta que se inicie este servicio. Si no dispone de los clientes IMAP4, puede deshabilitar este servicio.
Tipo de inicio	Manual
Contexto de seguridad	Sistema local
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Opcional

Back-end de Microsoft Exchange IMAP4

Información	Parámetros
Nombre corto	MSExchangeIMAP4BE
Descripción y dependencias	Recibe las conexiones de cliente IMAP4 procesadas por el proxy de la desde el acceso de cliente (frontend) servicio IMAP4. De forma predeterminada, este servicio no se está ejecutando, por lo que los clientes IMAP4 no se pueden conectar al servidor de Exchange hasta que se inicie este servicio. Si no dispone de los clientes IMAP4, puede deshabilitar este servicio.
Tipo de inicio	Manual
Contexto de seguridad	Servicio de red
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Opcional

Almacén de información de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeIS
Descripción y dependencias	Administra las bases de datos de buzones de correo en el servidor. Si este servicio se detiene, las bases de datos de buzones de correo en el servidor no están disponibles.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Topología de Active Directory de Microsoft Exchange Llamada a procedimiento remoto (RPC) Server Registro de eventos de Windows Estación de trabajo
Obligatorio u opcional	Obligatorio

Asistentes de buzón de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeMailboxAssistants
Descripción y dependencias	Realiza procesamiento en segundo plano de los buzones de correo en las bases de datos de buzones de correo en el servidor.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Obligatorio

Replicación de buzón de correo de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeMailboxReplication
Descripción y dependencias	Buzón de correo de los procesos se mueve y las solicitudes de movimiento.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Servicio de uso compartido Microsoft Exchange Active Directory TopologyNet.TCP puerto
Obligatorio u opcional	Obligatorio

Entrega de transporte de buzón de correo de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeDelivery
Descripción y dependencias	Recibe los mensajes SMTP desde el servicio de transporte de Microsoft Exchange (en los servidores de buzón de correo locales o remotos) y los entrega a una base de datos de buzón de correo local mediante RPC.
Tipo de inicio	Automático
Contexto de seguridad	Servicio de red
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Obligatorio

Envío de transporte de buzón de correo de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeSubmission
Descripción y dependencias	Recibe los mensajes RPC desde una base de datos de buzón de correo local y los envía a través de SMTP para el servicio de transporte de Microsoft Exchange (en los servidores de buzón de correo locales o remotos).
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Obligatorio

Agente de notificaciones de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeNotificationsBroker
Descripción y dependencias	Proporciona notificaciones de Exchange para los procesos de Exchange locales y remotas.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Topología de Active Directory de Microsoft Exchange Servicio de uso compartido de puertos Net.TCP
Obligatorio u opcional	Obligatorio

POP3 de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangePOP3
Descripción y dependencias	Los servidores proxy POP3 las conexiones cliente de los servicios de acceso de cliente (frontend) con el servicio back-end IMAP4 en los servidores de buzones. De forma predeterminada, este servicio no se está ejecutando, por lo que los clientes POP3 no se pueden conectar al servidor de Exchange hasta que se inicie este servicio.
Tipo de inicio	Manual
Contexto de seguridad	Servicio de red
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Opcional

Back-end de Microsoft Exchange POP3

Información	Parámetros
Nombre corto	MSExchangePOP3BE
Descripción y dependencias	Recibe las conexiones de cliente POP3 procesadas por el proxy de la desde el acceso de cliente (frontend) servicio POP3. De forma predeterminada, este servicio no se está ejecutando, por lo que los clientes POP3 no se pueden conectar al servidor de Exchange hasta que se inicie este servicio.
Tipo de inicio	Manual
Contexto de seguridad	Servicio de red
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Opcional

Servicio de replicación de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeRepl
Descripción y dependencias	Proporciona funcionalidad de replicación de bases de datos de buzones de correo en una base de datos de grupos de disponibilidad (dag).
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Obligatorio

Acceso de clientes RPC de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeRPC
Descripción y dependencias	Administra las conexiones de RPC de cliente de Exchange.
Tipo de inicio	Automático
Contexto de seguridad	Servicio de red
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Obligatorio

Búsqueda de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeFastSearch
Descripción y dependencias	Proporciona la indización de contenido de buzones de correo, lo que mejora el rendimiento de búsqueda de contenido.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Obligatorio

Controladora de Host de búsqueda de Microsoft Exchange

Información	Parámetros
Nombre corto	HostControllerService
Descripción y dependencias	Proporciona servicios de administración de aplicaciones y de implementación en el servidor de Exchange local.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Servicio HTTP
Obligatorio u opcional	Obligatorio

Extensión de servidor de Microsoft Exchange para la copia de seguridad de Windows Server

Información	Parámetros
Nombre corto	WSBExchange
Descripción y dependencias	Permite la copia de seguridad de Windows Server hacer una copia y restauración de datos de Exchange server.
Tipo de inicio	Manual
Contexto de seguridad	Sistema local
Dependencias	Ninguno
Obligatorio u opcional	Opcional

Host de servicio de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeServiceHost
Descripción y dependencias	Proporciona un servicio de host para los componentes de Exchange que no tengan sus propios servicios.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Obligatorio

Limitación de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeThrottling
Descripción y dependencias	Proporciona administración de carga de trabajo de usuario que limita la tasa de operaciones de usuario (anteriormente conocido como limitación de usuarios).
Tipo de inicio	Automático
Contexto de seguridad	Servicio de red
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Obligatorio

Transporte de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeTransport
Descripción y dependencias	Proporciona el servidor SMTP y la pila de transporte.
Tipo de inicio	Automático
Contexto de seguridad	Servicio de red
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Obligatorio

Búsqueda de registros de transporte de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeTransportLogSearch
Descripción y dependencias	Proporciona capacidades de búsqueda remota para los archivos de registro de transporte (por ejemplo, seguimiento de mensajes).
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Opcional

Mensajería (Exchange 2016 sólo) unificada de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeUM
Descripción y dependencias	Proporciona características de mensajería unificada (UM): permite que los mensajes de voz y fax deben almacenarse en Exchange 2016 y proporciona a los usuarios acceso telefónico a correo electrónico, correo de voz, calendario, contactos o un operador automático. Si este servicio se detiene, mensajería unificada no está disponible. Si no utiliza la mensajería unificada en ruta 2016, puede deshabilitar este servicio.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Aislamiento de claves CNG Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Opcional

Enrutador de llamada (sólo Exchange 2016) mensajería unificada de Microsoft Exchange

Información	Parámetros
Nombre corto	MSExchangeUMCR
Descripción y dependencias	Redirige las conexiones de cliente de mensajería unificada desde los servicios de acceso de cliente (frontend) para el servicio de mensajería unificada en los servidores de buzones de Exchange 2016 de back-end. Si no utiliza la mensajería unificada en Exchange 2016, puede deshabilitar este servicio.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Aislamiento de claves CNG Topología de Active Directory de Microsoft Exchange
Obligatorio u opcional	Opcional

Recuperación del administrador del estado de Microsoft Exchange

Información	Parámetros
Nombre corto	msexchangehmrecovery
Descripción y dependencias	Parte de la disponibilidad administrada que intenta recuperar componentes en mal estado en el servidor de Exchange.
Tipo de inicio	Automático
Contexto de seguridad	Sistema local
Dependencias	Registro de eventos de Windows Instrumental de administración de Windows
Obligatorio u opcional	Obligatorio

Puede obtener información adicional acerca de los servicios de Exchange Server 2016 a través de la siguiente dirección:

https://docs.microsoft.com/es-es/exchange/plan-and-deploy/deployment-ref/services-overview?view=exchserver-2016

6.3 SEGURIDAD DE DOMINIOS Y AUTENTICACIÓN MUTUA TLS

Desde Exchange Server 2010, Microsoft ha incorporado mecanismos que mejoran la confianza en el envío y recepción de mensajes de correo electrónico a través de redes no confiables o públicas como es internet. En este sentido, Exchange Server 2016 proporciona mecanismos avanzados de seguridad para proteger las conexiones SMTP desde o hacia servidores externos a la organización, en distintos niveles.

Dichos mecanismos se basan en 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.

Seguridad de nivel de transporte (TLS). Es un protocolo estándar que se usa para proporcionar comunicaciones Web seguras en Internet o en intranets. Permite a los clientes autenticar servidores y, opcionalmente, a los servidores autenticar clientes. También proporciona un canal seguro ya que cifra las comunicaciones. TLS 1.2 es la versión más reciente del protocolo Nivel de sockets seguros (SSL), aunque ya se está trabajando en la versión TLS 1.3.

TLS mutuo (M-TLS). TLS mutuo difiere de TLS en que el protocolo TLS normalmente se implementa para proporcionar confidencialidad en forma de cifrado, pero sin que se produzca autenticación entre el remitente y el destinatario. Es habitual en protocolos como HTTP donde sólo se autentica el servidor destinatario. Con la autenticación TLS mutua, cada servidor comprueba la identidad del otro servidor mediante la validación de un certificado proporcionado en cada extremo. De esta forma se puede garantizar la procedencia del mensaje y la integridad de éste, y esto se refleja en el cliente Microsoft Outlook mediante un ícono de dominio seguro:

a) **Seguridad de dominio.** Se denomina seguridad de dominio al conjunto de características, como la administración de certificados, la funcionalidad de conectores y el comportamiento del cliente de Outlook, que habilita la autenticación TLS mutua como una tecnología administrable en Exchange Server.

b) **TLS oportunista.** Exchange Server 2016 instala de forma predeterminada un certificado autofirmado que permite, entre otros aspectos, habilitar TLS oportunista desde el primer momento. Es por ello que, en entornos con servidores distribuidos, el envío y recepción de mensajes entre todos ellos se realiza de forma cifrada con SMTP sobre TLS. Además, se denomina TLS oportunista porque el servicio de transporte siempre va a intentar establecer una comunicación cifrada para todas las conexiones remotas antes de cambiar a una comunicación en claro.

c) **Confianza directa.** De forma predeterminada, todo el tráfico entre servidores de transporte perimetral y servidores de acceso de cliente se autentica y se cifra mediante M-TLS. En lugar de utilizar la validación X.509, Exchange Server 2016 utiliza la confianza directa para autenticar los certificados, lo cual significa que el certificado queda validado por su presencia en el servicio de Directorio Activo o el servicio Active Directory Lightweight Directory Services (AD LDS). Si se usa la confianza directa, no es determinante que el certificado tenga una firma personal o esté firmado por una entidad de certificación válida.

La seguridad de dominio en Exchange Server 2016 es una alternativa de bajo coste con respecto a S/MIME u otras soluciones de seguridad a nivel de mensajes, ya que se habilita para rutas y dominios concretos sobre los cuales se tiene una comunicación habitual, como por ejemplo socios externos, otros organismos públicos o instituciones colaboradoras.

Habilitando la seguridad de dominio se garantiza que el mensaje proviene de quien dice ser y que no ha sido modificado ni alterado en su transporte. Así mismo la comunicación es, en todo momento, confidencial y se reduce el riesgo de suplantación de identidad o envío de correo masivo no deseado en nombre de otra organización.

La seguridad de dominio usa la seguridad de la capa de transporte (TLS) con autenticación mutua (M-TLS) para proporcionar una autenticación y un cifrado basados en la sesión.

Exchange Server 2016 incluye un conjunto de comandos de PowerShell para crear, solicitar y administrar certificados TLS, los cuales de forma predeterminada son autofirmados.

Nota: Un certificado autofirmado es un certificado que firma su creador. En Exchange Server 2016, el certificado autofirmado se crea durante el proceso de instalación mediante la API de certificado (CAPI) subyacente de Windows. Los certificados autofirmados son menos confiables que los certificados generados por la infraestructura de claves públicas (PKI) o una entidad emisora de certificados (CA) de otros fabricantes.

Se recomienda usar certificados autofirmados sólo para el correo interno, aunque si las organizaciones de las cuales se recibe correo mediante dominio seguro utilizan certificados autofirmados y éstos se agregan manualmente al almacén de certificados raíz de confianza de cada servidor de transporte, los certificados autofirmados comenzarían a ser de confianza de forma explícita.

Para las conexiones que pasan por Internet, se recomienda generar certificados firmados por una PKI o una Entidad de Certificación de confianza de otros fabricantes. La generación de claves TLS con una la infraestructura de claves públicas (PKI) de confianza o una Entidad de Certificación (CA) de otros fabricantes reduce la administración necesaria para habilitar la seguridad de dominio.

6.4 FILTRADO DE TRANSPORTE Y AGENTES DE CONFORMIDAD

Muchas organizaciones están obligadas a procesar, filtrar, modificar y almacenar los mensajes de correo electrónico que se transfieren entre su organización e Internet y viceversa. La infraestructura de directivas de transporte y conformidad de Microsoft Exchange Server 2016 proporciona un conjunto de agentes y procesos que rigen el modo en que los mensajes de correo electrónico se almacenan y procesan en función de una serie de requisitos.

Así mismo, ya desde Microsoft Exchange Server 2013 Microsoft ha implementado una arquitectura que permite una independencia y mayor flexibilidad en la canalización del transporte, el cual, tal y como ya se ha indicado anteriormente, consta de los siguientes servicios:

a) Servicio de transporte front-end en servidores de acceso de cliente.

b) Servicio de transporte en servidores de buzones de correo.

c) Servicio de transporte de buzones en servidores de buzones de correo.

d) Servicio de transporte en servidores de transporte perimetral.

Debido a las actualizaciones realizadas en la canalización de transporte, los cmdlets de los agentes de transporte deben distinguir entre el servicio de transporte y el servicio de transporte front-end, especialmente si los servidores de acceso de cliente y de buzones de correo están instalados en el mismo equipo como es el caso en Exchange Server 2016.

Las siguientes características ayudan a las organizaciones a cumplir con los requisitos legales y de normativa con respecto a la gestión del correo electrónico:

a) Agentes de reglas de transporte. Los agentes de transporte utilizan eventos SMTP que se desencadenan a medida que los mensajes se desplazan por el canal de transporte. Dichos eventos dan a los agentes acceso a los mensajes en puntos específicos durante la conversación SMTP y durante el enrutamiento de los mensajes dentro de la organización.

b) Agente de registro en diario. Este agente ayuda a configurar la forma en que Exchange exige directivas de retención de correo electrónico en mensajes enviados o recibidos por departamentos o personas de la organización a destinatarios y de destinatarios fuera de la organización, o ambas combinaciones.

c) Agentes de cifrado y descifrado RMS. Los agentes RMS habilitan la capacidad de cifrado y descifrado automático durante el transporte de los mensajes, evitando así la necesidad de que sea el usuario el que cifre el mensaje con otras tecnologías más complejas para el usuario como S/MIME o PGP.

Así mismo, Exchange Server 2016 continúa incorporando el rol de servidor de transporte perimetral, el cual fortalece la seguridad en toda la cadena de transporte.

La instalación del servidor de transporte perimetral es opcional y puede ser reemplazado por un servicio de transporte SMTP estándar de otro fabricante o un servicio de pasarela online basado en la nube. El rol de transporte perimetral aporta una serie de características mejoradas que lo hacen muy recomendable en escenarios de medianas y grandes organizaciones, ya que ofrece una solución de transporte aislada del Directorio Activo, pero con administración centralizada gracias a la sincronización de objetos mediante el servicio EdgeSync.

En esta guía **no se contempla la instalación de rol de transporte perimetral**, sin embargo, sus funcionalidades de higiene de mensajes y control en el transporte no se pierden en su totalidad ya que se contempla su instalación de los agentes de transporte en el rol de servidor de buzones. Sin embargo, es importante destacar que algunos agentes no están disponibles fuera del rol de transporte perimetral.

En general, los agentes de transporte permiten realizar tareas de bloqueo, análisis y control de mensajes entrantes o salientes y aplicar reglas según las características de cada mensaje. Es decir, controlan el flujo de mensajes de acuerdo a reglas propias de la organización y facilita el cumplimiento de normas, leyes y directivas que obliguen a un tratamiento especial de los mensajes según sus características.

Los agentes de transporte se pueden definir como componentes de software administrados que realizan tareas en respuesta a un evento de aplicación.

Una de las principales ventajas de los agentes de transporte en la canalización del transporte es que se pueden registrar en cualquiera de los eventos SMTP y pueden actuar sobre una conexión, un mensaje o un contenido específico en un determinado momento.

Cuando un agente de transporte se configura, se asignan dos propiedades que determinan el orden de ejecución:

a) La prioridad de ejecución.

b) El evento SMTP que tiene asignado en la lista de eventos.

La prioridad se puede cambiar desde el Shell de Administración de Exchange, sin embargo, el momento en que finalmente el agente se ejecute va a estar dado por ambas propiedades.

Nota: Es muy importante tener en cuenta que: desde el 1 de noviembre de 2016, Microsoft ha dejado de desarrollar actualizaciones de definición de correo no deseado para los filtros de SmartScreen de Exchange y Outlook, incluyendo Exchange Server 2016. Las definiciones de spam SmartScreen existentes aún se pueden descargar, pero se reducirá en su eficacia a través del tiempo. Más información en: https://blogs.technet.microsoft.com/exchange/2016/09/01/deprecating-support-for-smartscreen-in-outlook-and-exchange/

En la siguiente tabla se observa la lista de agentes de transporte que el servidor de transporte perimetral instala por defecto, así como los eventos SMTP en los que se registran.

Nombre del agente	Prioridad	Eventos del categorizador o SMTP
Agente de filtro de conexión	1	OnConnectEvent, OnMailCommand, OnRcptComand, OnEndOfHeaders
Agente de reescritura de direcciones entrantes	2	OnRcptCommand, OnEndOfHeaders
Agente Regla perimetral	3	OnEndOfData
Agente de filtro de contenido	4	OnEndOfData
Agente de Id. de remitente	5	OnEndOfHeaders
Agente de filtro de remitentes	6	OnMailCommand, OnEndOfHeaders
Agente de filtro de destinatarios	7	OnRcptCommand
Agente de análisis de protocolo	8	OnEndOfHeaders, OnEndOfData, OnReject, OnRsetCommand, OnDisconnectEvent
Agente de filtro de documentos adjuntos	9	OnEndOfData
Agente de reescritura de direcciones salientes	10	OnSubmittedMessage, OnRoutedMessage

En la siguiente tabla se observa la lista de agentes de transporte que pueden ser instalados en el servidor de buzones de Exchange Server 2016. Estos agentes no se instalan de forma predeterminada.

Nombre del agente	Prioridad	Eventos SMTP
Agente de regla de transporte	1	OnResolvedMessage
Agente de malware	2	OnSubmittedMessage
Agente de enrutamiento de mensajes de texto	3	OnSubmittedMessage
Agente de entrega de mensajes de texto	4	N/D
Agente de registro en diario	No configurable	OnRoutedMessage
Agente de descifrado de informes de diario	No configurable	OnCategorizedMessage
Agente de descifrado de RMS	No configurable	OnSubmittedMessage
Agente de cifrado de RMS	No configurable	OnSubmittedMessage, OnRoutedMessage
Agente de descifrado de protocolo RMS	No configurable	OnEndOfData

La recepción de SMTP existe en el servicio de transporte perimetral en los servidores de acceso de cliente, el servicio de transporte en los servidores de buzones de correo y los servidores de transporte perimetral y el servicio de entrega de transporte de buzones en los servidores de buzones de correo. Sin embargo, el categorizador existe únicamente en el servicio de transporte en los servidores de buzones de correo y servidores de transporte perimetral.

La siguiente tabla incluye los eventos SMTP que proporcionan acceso a los mensajes en la canalización de transporte.

Secuencia	Evento SMTP	Descripción
Eventos de recepción SMTP		
1	OnConnectEvent	La conexión inicial desencadena este evento desde un host SMTP remoto.
2	OnHeloCommand	Este evento se desencadena cuando el host SMTP remoto emite el comando HELO.
3	OnEhloCommand	Este evento se desencadena cuando el host SMTP remoto emite el comando EHLO.
4	OnStartTlsCommand	Este evento se desencadena cuando el host SMTP remoto emite el comando STARTTLS.
5	OnAuthCommand	Este evento se desencadena cuando el host SMTP remoto emite el comando AUTH.
6	OnProcessAuthentication	Este evento se desencadena cuando se procesa la autenticación con el host SMTP remoto.
7	OnEndOfAuthentication	Este evento se desencadena cuando el host SMTP remoto ha completado la autenticación.
8	OnXSessionParamsCommand	Este evento se desencadena cuando el host SMTP remoto emite el comando XSESSIONPARAMS.
9	OnMailCommand	Este evento se desencadena cuando el host SMTP remoto emite el comando MAIL FROM.
10	OnRcptToCommand	Este evento se desencadena cuando el host SMTP remoto emite el comando RCPT TO.
11	OnDataCommand	Este evento se desencadena cuando el host SMTP remoto emite el comando DATA (texto) o BDAT (datos binarios).
12	OnEndOfHeaders	Este evento se desencadena cuando el host SMTP remoto ha completado el envío de encabezados de mensajes de correo electrónico. Esto se indica con una línea en blanco (<CRLF>) que separa los encabezados de mensajes y los cuerpos de mensajes.
13	OnProxyInboundMessage	Este evento se desencadena cuando el servicio de transporte front-end retransmite o envía por proxy una sesión SMTP entrante en un servidor de acceso de cliente al servicio de transporte de un servidor de buzones de correo.
14	OnEndOfData	Este evento se desencadena cuando el host SMTP remoto emite un comando de fin de datos. En el caso de las sesiones de texto que inicia el comando DATA, el indicador de fin de datos es <CRLF>.<CRLF>. En el caso de las sesiones binarias que inicia el comando BDAT, el indicador de fin de datos es BDAT LAST.
**	OnHelpCommand	Este evento se desencadena si el host SMTP remoto emite el comando HELP.
**	OnNoopCommand	Este evento se desencadena si el host SMTP remoto emite el comando NOOP.
**	OnReject	Este evento se desencadena si el host SMTP de recepción emite un código de notificación de estado de entrega (DSN) temporal o permanente al host SMTP emisor.

Secuencia	Evento SMTP	Descripción
**	OnRsetCommand	Este evento se desencadena si el host SMTP de envío emite el comando RSET.
15	OnDisconnectEvent	Este evento se desencadena cuando el host SMTP de envío o de recepción se desconecta de la conversación SMTP. Por lo general, esto sucede cuando el host SMTP remoto emite el comando QUIT.
5	OnAuthCommand	Este evento se desencadena cuando el host SMTP remoto emite el comando AUTH.

Nota: ** Estos eventos pueden producirse en cualquier momento después de OnConnectEvent pero antes de OnDisconnectEvent.

A continuación, se muestran los eventos del categorizador.

Secuencia	Evento SMTP	Descripción
Eventos de categorizador		
1	OnSubmittedMessage	Este evento se desencadena cuando un mensaje llega en la cola de envío en el servicio de transporte en el servidor de buzones de correo de recepción o el servidor de transporte perimetral.
2	OnResolvedMessage	Este evento se desencadena una vez que se han resuelto todos los destinatarios, pero antes de que se determine el siguiente salto para cada uno de ellos. El evento de enrutamiento OnResolvedMessage permite que los eventos de enrutamiento posteriores invaliden el comportamiento de enrutamiento predeterminado mediante la utilización del método por destinatario SetRoutingOverride.
3	OnRoutedMessage	Este evento se desencadena una vez que los mensajes se han categorizado, las listas de distribución se han expandido y se han resuelto los destinatarios.
4	OnCategorizedMessage	Este evento se desencadena cuando el categorizador finaliza el procesamiento del mensaje.

Desde el punto de vista de la prioridad de ejecución, existen dos factores que determinan el orden en el que actúan los agentes de transporte en los mensajes en la canalización de transporte:

a) El evento SMTP en el que se registra el agente de transporte y cuando el evento SMTP encuentra mensajes.

b) El valor de prioridad que se asigna al agente de transporte si hay varios agentes registrados en el mismo evento SMTP. La prioridad más alta es 1. Un valor entero más alto indica una prioridad de agente más baja.

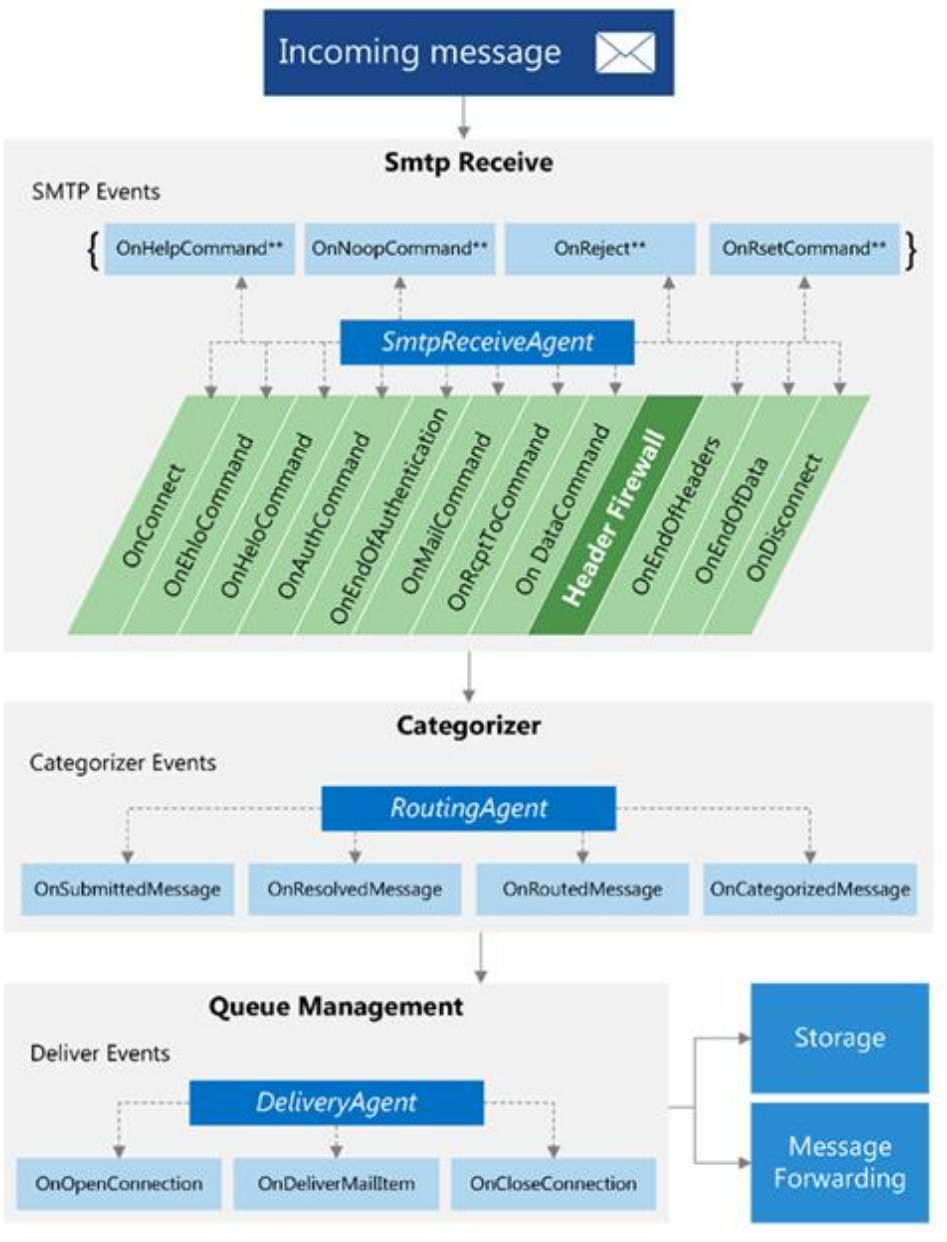
Para luchar contra el correo electrónico no deseado, la consideración más importante, además de la validez de los contenidos del mensaje, es el momento en el que se identifica y rechaza un mensaje de correo electrónico no deseado válido.

Es importante saber que, cuanto antes se rechace un mensaje que se ha confirmado como no deseado, menor será el coste para la organización.

Por otro lado, para los agentes antivirus, la consideración más importante es asegurarse de que se examinan todos los mensajes. Los agentes que deben examinar todos los mensajes tienen que estar configurados en el evento OnSubmittedMessage.

Los mensajes que fluyen a través del canal de transporte encuentran el evento SMTP OnSubmittedMessage porque éste tiene lugar después de todos los puntos de entrada de envío, como el envío SMTP desde host remotos, envíos MAPI desde equipos que ejecutan la función del servidor Buzón de correo, el directorio Pickup que utilizan las aplicaciones personalizadas, o el directorio Replay que utilizan las aplicaciones de correo electrónico de terceros.

A continuación, se muestra una imagen (en inglés) procedente de Microsoft Technet donde se observan las relaciones entre los componentes de la canalización del transporte de Exchange Server 2016, así como los diferentes eventos SMTP y del categorizador.



Los mensajes procedentes de fuera de la organización entran a la canalización de transporte a través del conector de recepción en el servicio de transporte front-end en un servidor de acceso de clientes y luego se encaminan al servicio de transporte en el servidor de buzones de correo.

Si la organización dispone de un servidor de transporte perimetral de Exchange Server 2016 instalado en la red perimetral, los mensajes que entran desde fuera de la organización llegan a la canalización de transporte a través del conector de recepción en el servicio de transporte en el servidor perimetral. El servidor de acceso de cliente se usa para el flujo de correo entrante. El flujo de correo se produce desde el servicio de transporte en el servidor perimetral al servicio de transporte front-end en el servidor de acceso de clientes, y después al servicio de transporte en el servidor de buzones de correo.

Así mismo, a diferencia de versiones anteriores, cada mensaje que se envía o recibe mediante un cliente Exchange Server 2016 debe categorizarse en un servidor de buzones antes de que se encamine y se entregue.

Desde la arquitectura de Exchange Server 2013, el servidor de acceso de clientes no realiza funciones de categorizador, únicamente reenvía el mensaje al siguiente servidor de buzones disponible en un modelo de alta disponibilidad y redundancia.

Si el mensaje tiene destinatarios externos a la organización, el mensaje se enruta desde el servicio de transporte en el servidor de buzones de correo a Internet, o desde el servidor de buzones de correo al servicio de transporte front-end en un servidor de acceso de clientes y después a Internet si el conector de envío está configurado para redirigir las conexiones salientes mediante proxy a través del servidor de acceso de clientes.

Es importante tener en cuenta que, si la organización dispone de un servidor de transporte perimetral instalado en la red perimetral, los mensajes con destinatarios externos nunca se envían a través del servicio de transporte front-end en un servidor de acceso de clientes. El mensaje se envía desde el servicio de transporte de un servidor de buzones de correo al servicio de transporte del servidor de transporte perimetral.

Nota: Al implementar Exchange Server 2016, no se puede realizar un envío de correo saliente hasta que se configure un conector de envío para encaminar el correo saliente hacia Internet.

Los componentes del servicio de transporte en los servidores de transporte perimetral son idénticos a los componentes del servicio de transporte en los servidores de buzones de correo.

No obstante, lo que realmente sucede durante cada fase del procesamiento en los servidores de transporte perimetral es distinto. Dichas diferencias se describen a continuación:

a) **Recepción SMTP.** Cuando un servidor de transporte perimetral se suscribe a un sitio interno de Directorio Activo, el conector de recepción predeterminado se configura automáticamente para aceptar correo de los servidores de buzones de correo internos y de Internet. Cuando llegan mensajes de Internet al servidor de transporte perimetral, los agentes contra correo no deseado filtran las conexiones y el contenido de los mensajes, y ayudan a identificar el remitente y el destinatario.

Nota: Los agentes contra correo no deseado están instalados y habilitados de manera predeterminada en los servidores de transporte perimetral y aunque incluyen otras características de filtrado de conexión y filtrado de datos adjuntos, no tienen capacidades integradas de filtrado de código dañino.

b) **Envío.** En un servidor de transporte perimetral, los mensajes entran normalmente a la cola de envío a través del conector de recepción. Sin embargo, el directorio de recogida y el directorio de reproducción también están disponibles.

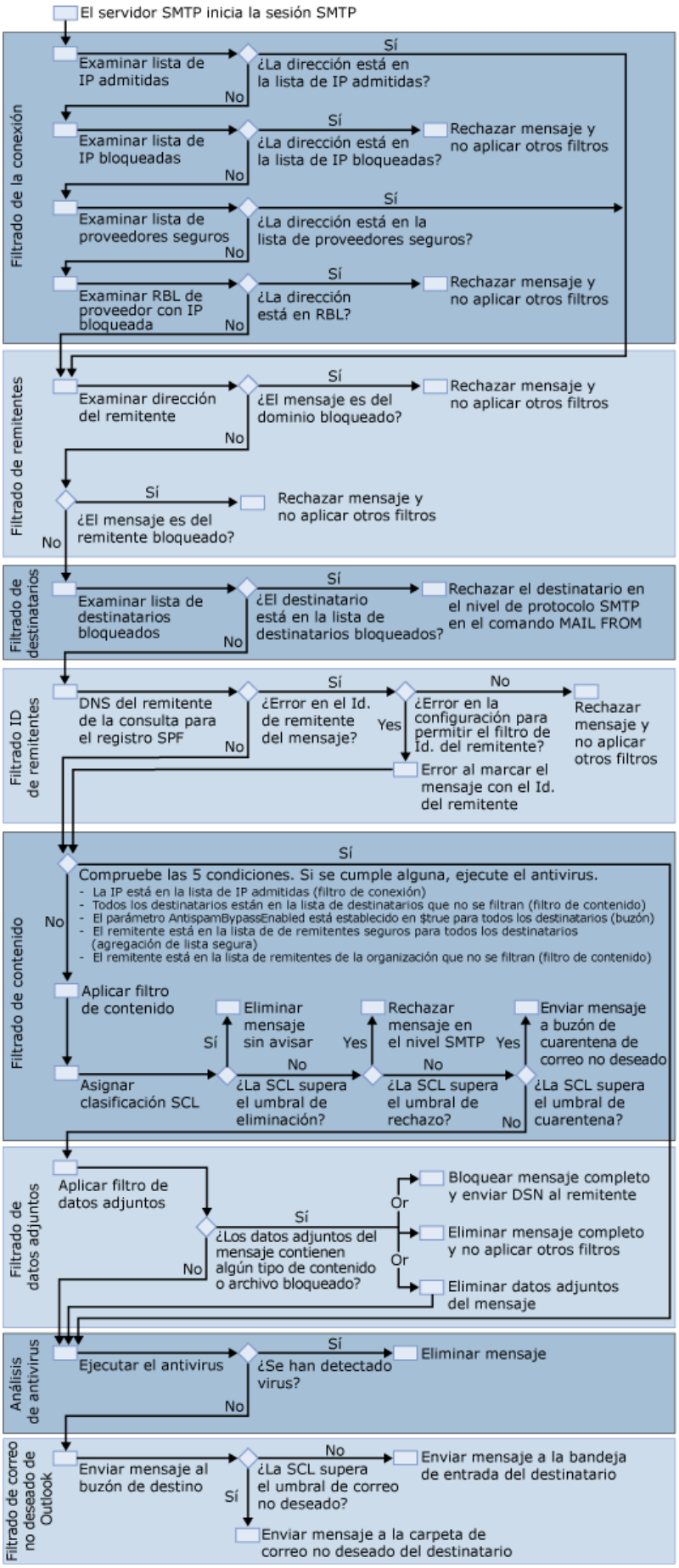
c) **Categorizador.** En un servidor de transporte perimetral, la categorización es un proceso breve en el que el mensaje se pone directamente en una cola de entrega para entrega a los destinatarios internos o externos.

d) **Envío SMTP.** Cuando un servidor de transporte perimetral se suscribe a un sitio interno de Directorio Activo, se crean y configuran automáticamente dos conectores de envío. Uno es responsable de enviar correo saliente a los destinatarios de Internet, mientras que el otro es responsable de enviar correo entrante de Internet a los destinatarios internos. El correo entrante se envía al servicio de transporte en un servidor de buzones de correo disponible en el sitio de Directorio Activo al cual está suscrito el servidor perimetral.

Desde el punto de vista de la lucha contra el correo electrónico no deseado, cuando un usuario externo envía mensajes de correo electrónico a un servidor de Microsoft Exchange 2016 en el que se ejecutan agentes de transporte contra correo electrónico no deseado, éstos evalúan de forma acumulativa los atributos de los mensajes entrantes y, o bien filtran los mensajes sospechosos de ser correo electrónico no deseado, o les asignan una clasificación basada en la probabilidad de que lo sean.

Esta clasificación se almacena con el mensaje como una propiedad extendida denominada clasificación de nivel de confianza contra correo no deseado (SCL) y se conserva con el mensaje cuando éste se envía a otros servidores de Exchange.

A continuación, se muestra el orden en que los agentes de transporte contra el correo electrónico no deseado y el análisis frente a código dañino integrado en Exchange Server 2016 filtran los mensajes de correo electrónico procedentes de Internet o conexiones no autenticadas (no confiables).


El servidor SMTP inicia la sesión SMTP
Filtrado de la conexión
Examinar lista de IP admitidas
¿La dirección está en la lista de IP admitidas?
Sí
No
Examinar lista de IP bloqueadas
¿La dirección está en la lista de IP bloqueadas?
Rechazar mensaje y no aplicar otros filtros
Examinar lista de proveedores seguros
¿La dirección está en la lista de proveedores seguros?
Examinar RBL de proveedor con IP bloqueada
¿La dirección está en RBL?
Filtrado de remitentes
Examinar dirección del remitente
¿El mensaje es del dominio bloqueado?
¿El mensaje es del remitente bloqueado?
Filtrado de destinatarios
Examinar lista de destinatarios bloqueados
¿El destinatario está en la lista de destinatarios bloqueados?
Rechazar el destinatario en el nivel de protocolo SMTP en el comando MAIL FROM
Filtrado ID de remitentes
DNS del remitente de la consulta para el registro SPF
¿Error en el Id. de remitente del mensaje?
¿Error en la configuración para permitir el filtro de Id. del remitente?
Yes
Rechazar mensaje y no aplicar otros filtros
Error al marcar el mensaje con el Id. del remitente
Filtrado de contenido
Compruebe las 5 condiciones. Si se cumple alguna, ejecute el antivirus.
- La IP está en la lista de IP admitidas (filtro de conexión)
- Todos los destinatarios están en la lista de destinatarios que no se filtran (filtro de contenido)
- El parámetro AntispamBypassEnabled está establecido en $true para todos los destinatarios (buzón)
- El remitente está en la lista de de remitentes seguros para todos los destinatarios (agregación de lista segura)
- El remitente está en la lista de remitentes de la organización que no se filtran (filtro de contenido)
Aplicar filtro de contenido
Asignar clasificación SCL
Eliminar mensaje sin avisar
¿La SCL supera el umbral de eliminación?
Rechazar mensaje en el nivel SMTP
¿La SCL supera el umbral de rechazo?
Enviar mensaje a buzón de cuarentena de correo no deseado
¿La SCL supera el umbral de cuarentena?
Filtrado de datos adjuntos
Aplicar filtro de datos adjuntos
¿Los datos adjuntos del mensaje contienen algún tipo de contenido o archivo bloqueado?
Or
Bloquear mensaje completo y enviar DSN al remitente
Eliminar mensaje completo y no aplicar otros filtros
Eliminar datos adjuntos del mensaje
Análisis de antivirus
Ejecutar el antivirus
¿Se han detectado virus?
Eliminar mensaje
Filtrado de correo no deseado de Outlook
Enviar mensaje al buzón de destino
¿La SCL supera el umbral de correo no deseado?
Enviar mensaje a la bandeja de entrada del destinatario
Enviar mensaje a la carpeta de correo no deseado del destinatario

Los agentes contra correo no deseado se habilitan en un servidor de buzones de correo cuando la organización no tiene ningún servidor de transporte perimetral o el correo electrónico no deseado no se filtra antes de aceptar mensajes entrantes.

Al igual que el resto de agentes de transporte, a los agentes contra correo electrónico no deseado se les asigna un valor de prioridad determinado. Un valor bajo indica una prioridad alta, por lo que, en general, un agente contra correo no deseado con la prioridad 1 actuará sobre un mensaje antes que otro agente con la prioridad 9. No obstante, el evento SMTP en el que se registra el agente contra correo electrónico no deseado también es muy importante a la hora de determinar el orden en el que los agentes contra correo no deseado actúan sobre los mensajes. Un agente contra correo no deseado con prioridad baja que se registre en un evento SMTP con anterioridad en la canalización del transporte actuará antes sobre un mensaje que un agente con prioridad alta que se haya registrado posteriormente en el evento SMTP en la canalización de transporte.

En la siguiente lista se muestran los agentes contra correo no deseado en los servidores de buzones de correo y el orden predeterminado en el que se aplican a los mensajes en función del valor de prioridad predeterminado y del evento SMTP de la canalización de transporte:

a) Agente de filtrado de remitentes.

b) Agente de Id. de remitente.

c) Agente de filtro de contenido.

d) Agente de análisis de protocolo y reputación del remitente.

Por el contrario, si en su organización hay un servidor de transporte perimetral instalado en la red perimetral, todos los agentes contra correo no deseado que están disponibles en un servidor de buzones de correo se instalan y se habilitan de forma predeterminada en el servidor de transporte perimetral.

Además, los siguientes agentes contra correo no deseado solo están disponibles en un servidor de transporte perimetral:

a) Agente de filtrado de conexión.

b) Agente de filtrado de destinatarios.

c) Agente de filtrado de datos adjuntos.

Por lo tanto, a continuación, se muestra el orden completo en el que los agentes contra correo no deseado se aplican en un servidor de transporte perimetral:

a) Agente de filtro de conexión.

b) Agente de filtro de remitentes.

c) Agente de filtro de destinatarios.

d) Agente de Id. de remitente.

e) Agente de filtro de contenido.

f) Agente de análisis de protocolo y reputación del remitente.

g) Agente de filtrado de datos adjuntos.

6.4.1 AGENTE DE FILTRO DE CONEXIÓN

El filtrado de conexiones es una característica contra correo no deseado en Microsoft Exchange Server 2016 que admite o bloquea correo electrónico según el origen del mensaje.

El agente de filtrado de conexiones lleva a cabo el filtrado de conexiones, el cual está disponible solo en los servidores de transporte perimetral y se basa en la dirección IP del servidor que realiza la conexión para determinar la acción, que se realiza en un mensaje entrante.

De forma predeterminada, este es el primer agente contra correo no deseado en evaluar un mensaje entrante en un servidor de transporte perimetral. La dirección IP de origen de la conexión SMTP se comprueba según la lista de direcciones IP permitidas y bloqueadas.

Si la dirección IP de origen se ha permitido de forma explícita, el mensaje se envía a los destinatarios de la organización sin que otros agentes contra correo no deseado lleven a cabo ningún procesamiento adicional.

Si la dirección IP de origen se ha bloqueado de forma explícita, la conexión SMTP se cancelará. Si la dirección IP de origen no se ha permitido o bloqueado de forma explícita, el mensaje fluye a través de los demás agentes contra correo no deseado en el servidor de transporte perimetral.

El agente compara la dirección IP del servidor de correo de origen con los valores en la lista de direcciones IP permitidas, la lista de direcciones IP bloqueadas, los proveedores de la lista de IP permitidas y los proveedores de la lista de IP bloqueadas. Es necesario configurar al menos uno de estos cuatro almacenes de datos de direcciones IP para que el filtrado de conexiones evalúe la dirección IP del servidor de origen.

6.4.2 AGENTE DE FILTRO DE REMITENTES

El filtrado de remitentes se basa en el encabezado "MAIL FROM:", el cual determina qué acción, si la hay, se debería realizar en un mensaje de correo electrónico de entrada.

El agente de filtro de remitentes actúa sobre los mensajes de remitentes específicos ajenos a la organización. Los administradores de la organización pueden mantienen una lista de remitentes que se bloquean para que no envíen mensajes a la organización.

Se pueden bloquear a remitentes individuales (como usuario@dominio.com), dominios enteros (dominio.com) o dominios y todos sus subdominios (*.dominio.com).

También se puede configurar qué acción realizará el agente de filtro de remitentes cuando se encuentra un mensaje de un remitente bloqueado. Para ello, se pueden configurar las siguientes acciones:

a) El agente de filtro de remitentes rechaza la solicitud de SMTP con un error de sesión SMTP "554 5.1.0 remitente denegado" y cierra la conexión.

b) El agente de filtro de remitentes acepta el mensaje y lo actualiza para indicar que proviene de un remitente bloqueado. Dado que el mensaje proviene de un remitente bloqueado y está marcado como tal, el agente de filtro de contenido usará esta información cuando calcule el nivel de confianza de correo no deseado (SCL).

Nota: Como bien es sabido, los encabezados SMTP en general y particularmente MAIL FROM se pueden suplantar o alterar, por tanto, la estrategia antispam no debe basarse únicamente en el agente de filtro de remitentes. Se recomienda utilizar el agente de filtro de remitentes y el agente de identificación de remitentes en conjunto ya que el agente de identificación del remitente usa la dirección IP de origen del servidor de envío para verificar que el dominio registrado en MAIL FROM coincide con el dominio registrado en los servidores DNS.

Cuando el agente de filtro de remitentes está habilitado en un servidor de Exchange, el filtrado de remitentes bloquea los mensajes entrantes que provienen de Internet pero que no están autenticados. Estos mensajes se consideran mensajes externos.

6.4.3 AGENTE DE FILTRO DE DESTINATARIOS

El filtrado de destinatarios es una característica de Microsoft Exchange Server contra el correo no deseado que usa el encabezado "RCPT TO" para determinar qué acción, en caso de que sea necesario, se realizará en un mensaje de correo electrónico entrante.

El agente de filtro de destinatarios bloquea los mensajes en función de las características del destinatario de la organización y puede ayudar a impedir la aceptación de mensajes en los siguientes escenarios:

a) **Destinatarios no existentes.** Puede impedir la entrega a destinatarios que no estén en la libreta de direcciones de la organización.

b) **Listas de distribución restringidas.** Puede impedir la entrega de correo de Internet a listas de distribución que solo deben usar los usuarios internos.

c) **Buzones de correo que no deben recibir mensajes de Internet.** Puede impedir la entrega de correo de Internet a un buzón o alias específico que se suela usar dentro de la organización, como el departamento de soporte técnico.

El agente de filtro de destinatarios actúa en los destinatarios almacenados en una o las dos fuentes de datos siguientes:

a) **Lista de destinatarios bloqueados.** Esta es una lista definida por un administrador de los destinatarios que no deben recibir nunca mensajes de Internet.

b) **Búsqueda de destinatarios.** Son consultas en Directorio Activo para comprobar si el destinatario existe en la organización. En un servidor de transporte perimetral, la búsqueda de destinatarios requiere el acceso a información de Directorio Activo proporcionada por el servicio EdgeSync a la instancia local de Active Directory Lightweight Directory Services (AD LDS).

Si se habilita el agente de filtro de destinatarios, se realiza una de las acciones siguientes en los mensajes entrantes según las características de los destinatarios. Dichos destinatarios los indica el encabezado RCPT TO.

a) Si el mensaje entrante contiene un destinatario que está en la lista de destinatarios bloqueados, el servidor Exchange envía un error de sesión SMTP "550 5.1.1 Usuario desconocido" al servidor remitente.

b) Si el mensaje entrante contiene un destinatario que no coincide con ninguno de los de la búsqueda de destinatarios, el servidor Exchange envía un error de sesión SMTP "550 5.1.1 Usuario desconocido" al servidor remitente.

c) Si el destinatario no está en la lista de destinatarios bloqueados, pero sí aparece en la búsqueda de destinatarios, el servidor Exchange envía una respuesta SMTP "250 2.1.5 Recipient OK" al servidor remitente y el siguiente agente contra correo electrónico no deseado de la cadena procesa el mensaje.

Con respecto a la opción de bloqueo de mensajes dirigidos a destinatarios que no estén en la libreta global de direcciones (GAL), se tiene que tener en cuenta que si se habilita esta opción y no se configura adecuadamente el parámetro "Tar-Pit", se tiene un cierto riesgo de sufrir un ataque DHA (Directory Harvesting Attack).

Los ataques DHA son ataques por fuerza bruta que consisten en el envío masivo de mensajes a direcciones de la organización utilizando combinaciones de caracteres y números. Todos aquellos intentos que reciban una respuesta REJECT de SMTP (rechazo) por parte del servidor, se descartarán. Aquellos intentos que en los que no se reciba dicha respuesta, se considerará que se ha encontrado una combinación válida para una dirección SMTP de la organización que está siendo atacada.

En relativamente poco tiempo, se podría extraer mediante esta técnica todo el directorio de la organización. Es por ello que, con el fin de minimizar este riesgo, Microsoft Exchange implementa una contramedida denominada "Tar-Pitting" de forma integrada en los conectores de recepción.

El retraso del tráfico de red hace que los ataques de robo de directorio sean demasiado costosos como para automatizarlos eficazmente.

Las técnicas de envío de correo no deseado se basan fundamentalmente en la capacidad de envío del mayor número de mensajes en el menor tiempo posible.

Es recomendable especificar intervalos de retraso del tráfico de red pequeños mientras se analiza el resultado en términos de protección y rendimiento. De forma predeterminada Exchange Server 2016 implementa un retraso de 5 segundos en todos los conectores de recepción.

Nota: Se recomienda configurar con cuidado el valor "Tar-Pti". Un intervalo demasiado largo podría interrumpir el flujo de correo legítimo, mientras que uno demasiado corto podría no ser tan eficaz a la hora de frustrar un ataque por recolección de directorios. Si decide cambiar el intervalo de retraso del tráfico de red, es recomendable hacerlo en incrementos pequeños mientras se comprueban los resultados.

6.4.4 AGENTE DE FILTRO DE IDENTIFICACIÓN DE REMITENTE

Una vez procesado el mensaje por el agente de filtro de destinatarios, el siguiente agente en actuar es el agente de identificación de remitente o Sender ID.

Sender ID es una tecnología desarrollada y promovida por Microsoft, basada en la definición SPF (Sender Policy Framework) y en una tecnología anterior llamada Caller ID. Múltiples productos y organizaciones incorporan Sender ID como parte de sus sistemas de protección, entre ellos Sendmail, Symantec, Barracuda Networks e IronPort de Cisco.

Microsoft ha definido Sender ID como una tecnología libre de royalties, incluyéndola en su licencia Open Specification Promise.

Nota: Si lo desea, puede consultar el detalle del licenciamiento y las condiciones de uso de la tecnología Sender ID en la siguiente URL: http://www.microsoft.com/en-us/news/press/2006/oct06/10-23OSPSenderIDPR.aspx

Es por ello que cualquier fabricante de software o de tecnologías anti SPAM puede utilizar Sender ID sin ningún coste de licenciamiento.

Sender ID Framework es una tecnología de identificación que ayuda a determinar la legitimidad del remitente, verificando el dominio y la IP desde la cual se ha enviado el mensaje. Aunque indirectamente ayuda a reducir el SPAM, el principal objetivo de Sender ID es la reducir la suplantación de identidad y el Phising.

Además, Sender ID introduce el concepto de PRA (Purported Responsible Address), el cual es una dirección que se obtiene analizando los encabezados del mensaje asociados al reenvío del mensaje (resent-sender). Habitualmente el cliente Outlook reconoce estos encabezados incorporando el texto "Send on behalf of" o "Enviado en nombre de" al título del mensaje.

Lo primero que hace el agente de Sender ID en Exchange Server es determinar la dirección PRA (Purported Responsible Address) del mensaje, utilizando el algoritmo definido en el documento técnico RFC 4407.

La detección de la dirección PRA no garantiza que el mensaje provenga de quien dice ser, ya que los encabezados SMTP son fácilmente modificables.

Con la información PRA y FROM, el agente de filtro de Sender ID hace una consulta DNS al dominio remitente, para identificar si la IP desde la cual ha sido enviado el mensaje está autorizada como MTA (Mail Transfer Agent) para dicho dominio. Para poder realizar dicha consulta, el administrador del dominio remitente debe haber publicado previamente en los servidores DNS un registro de tipo texto denominado SPF.

En el registro SPF se indican los servidores, direcciones IP y dominios válidos que se envían desde dichas IPs. Si se recibe algún mensaje que dice ser del dominio remitente, pero enviado desde una IP no autorizada, entonces el agente Sender ID puede realizar alguna de las siguientes acciones:

a) Rechazar el mensaje. Se envía un mensaje de rechazo de protocolo SMTP con código 5xx.

b) Eliminar el mensaje. Se acepta el mensaje con un falso OK, pero inmediatamente lo elimina.

c) Marcar el mensaje y seguir su procesamiento. Se crea un encabezado con el resultado de la validación Sender ID, el cual se utilizará posteriormente para calcular el valor de confidencia de SPAM por parte del agente de filtro de contenido. Esta es la opción predeterminada.

El proceso de evaluación del identificador del remitente genera un estado para el mensaje, el cual se utiliza para evaluar posteriormente la clasificación SCL del mensaje. Este estado se puede establecer en uno de los siete valores siguientes.

Resultado de Sender ID	Descripción	Acción
Neutral	Los datos de identificación del remitente publicados no son concluyentes explícitamente y por lo tanto no se toman decisiones.	Registrar y aceptar
Pass (+)	La dirección IP de la dirección de responsabilidad supuesta (PRA) está en el conjunto permitido.	Registrar y aceptar

Resultado de Sender ID	Descripción	Acción
Fail (-) – El dominio no existe – Remitente no permitido – Dominio mal formado – Encabezado sin PRA	La dirección IP no está permitida, no se encontró ninguna dirección PRA en el correo entrante o no existe el dominio del remitente.	Registrar y aceptar, después eliminar o rechazar.
Soft Fail (~)	Es posible que la dirección IP de la dirección de responsabilidad supuesta (PRA) no esté en el conjunto permitido.	Registrar y aceptar
None	No existe entrada SPF publicada en el DNS del dominio.	Registrar y aceptar
TempError	Hay un error temporal, como que un servidor DNS no está disponible.	Registrar y aceptar
Perm Error	Hay un error irrecuperable, como puede ser un error en el formato de los registros y no se pueden leer correctamente.	Registrar y aceptar

El estado de la identificación del remitente se agrega a los metadatos del mensaje y posteriormente se convierte en una propiedad de MAPI. El filtro de correo electrónico no deseado de Microsoft Office Outlook utiliza la propiedad MAPI durante la creación del valor del nivel de confianza de correo no deseado (SCL).

El nivel de confianza de correo no deseado (SCL) del mensaje muestra la clasificación del mensaje en función de su contenido. El valor de SCL se encuentra entre 0 y 9, donde 0 indica que es poco probable que sea correo electrónico no deseado y 9 indica que es más probable que sea correo electrónico no deseado. Las acciones que Exchange Server y Outlook realizan dependen de la configuración de los umbrales de SCL.

6.4.5 AGENTE DE FILTRO DE CONTENIDO

El agente de filtro de contenido constituye una evolución del antiguo filtro inteligente de mensajes (IMF) que ya se incluía en Exchange Server 2003.

Nota: Es muy importante tener en cuenta que: desde el 1 de noviembre de 2016, Microsoft ha dejado de desarrollar actualizaciones de definición de correo no deseado para los filtros de SmartScreen de Exchange y Outlook, incluyendo Exchange Server 2016. Las definiciones de spam SmartScreen existentes aún se pueden descargar, pero se reducirá en su eficacia a través del tiempo. Más información en: https://blogs.technet.microsoft.com/exchange/2016/09/01/deprecating-support-for-smartscreen-in-outlook-and-exchange/

A diferencia de otras tecnologías de filtrado, el agente de filtro de contenido utiliza características de una importante muestra estadística de mensajes de correo electrónico.

La inclusión de mensajes legítimos en esta muestra reduce la posibilidad de errores y, debido a que el agente de filtro de contenido reconoce las características de los mensajes inofensivos y del correo no deseado, su exactitud aumenta.

El agente de filtro de contenido asigna una clasificación de confianza de correo no deseado (SCL) a cada mensaje, en un intervalo entre 0 y 9. Una clasificación SCL alta indica que el mensaje tiene más posibilidades de ser correo no deseado.

Sin embargo, antes de que el agente de filtro de contenido actúe calculando los niveles de confianza de correo no deseado (SCL), debe tomar ciertas decisiones basándose en 5 condiciones previas:

a) La dirección IP del remitente se encuentra en la lista de IP permitidas para filtrado de conexiones.

b) Todos los destinatarios se encuentran en la lista de excepciones para filtrado de contenido.

c) El parámetro "AntiSpamBypassEnabled" está establecido en "$True" en todos los buzones de correo de los destinatarios.

d) Todos los destinatarios han agregado a este remitente a su lista de remitentes seguros de Microsoft Outlook, que se actualiza en el servidor de transporte perimetral mediante la adición de listas seguras.

e) El remitente es un asociado de confianza y se encuentra en la lista de remitentes de la organización que no se filtran.

Si alguna de estas condiciones es verdadera, entonces el filtro de contenido no se aplica y se pasaría el mensaje al siguiente agente.

Nota: El filtro inteligente de mensajes no analiza los mensajes que superan los 11 MB. En su lugar, pasan a través del filtro de contenido sin que se examinen.

Así mismo, se pueden establecer excepciones al filtrado para aquellos usuarios (remitentes o destinatarios) que por la naturaleza de su trabajo requieren que el correo electrónico no se filtre, por ejemplo, analistas de seguridad, investigadores de delitos telemáticos, periodistas, etc.

Además, es posible configurar que no se aplique el agente de filtro de contenido a aquellas conexiones SMTP autenticadas, por ejemplo, las que provienen desde un socio de la organización. Para ello, se debe establecer el permiso "Ms-Exch-Bypass-Anti-Spam" en el conector utilizado por los socios.

El permiso para eludir el filtro contra correo electrónico no deseado no se concede a los socios de forma predeterminada y debe asignarlo un administrador.

Como se ha indicado anteriormente, el agente de filtro de contenido funciona calculando un valor de confianza de correo electrónico no deseado (SCL) en todos los mensajes entrantes después de que otros agentes contra correo electrónico no deseado hayan procesado los mensajes entrantes.

Muchos de los otros agentes contra correo electrónico no deseado que procesan los mensajes entrantes antes de que sean procesados por el agente de filtro de contenido determinan su forma de actuar sobre un mensaje.

Como el filtrado de contenido no es un proceso exacto y determinista, es importante ajustar adecuadamente la acción que realiza el agente de filtrado de contenido en los diferentes valores del nivel de confianza de correo no deseado.

Existen tres umbrales que se pueden configurar en este agente:

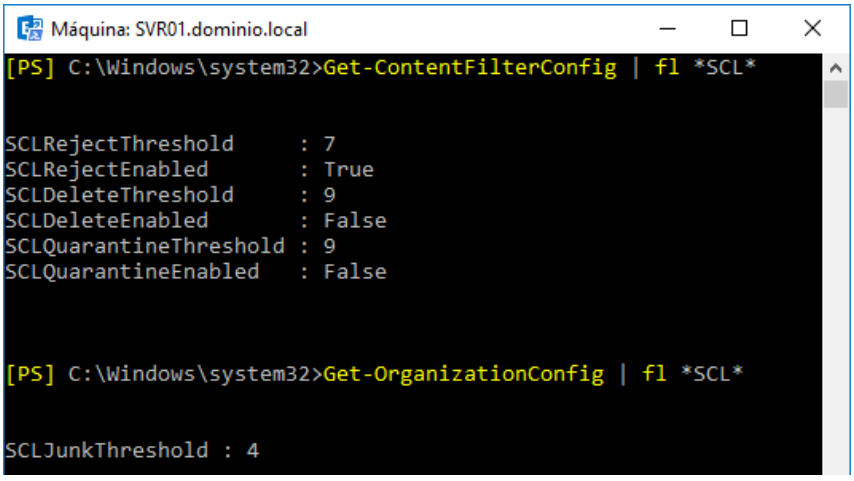
a) **Umbral de eliminación SCL.** Si el valor de SCL de un mensaje determinado es igual o superior al umbral de eliminación SCL, el agente de filtro de contenido elimina el mensaje. No hay ninguna comunicación en el nivel de protocolo que indique al sistema de envío o al remitente que el mensaje se ha eliminado. Si el valor SCL de un mensaje es inferior al valor del umbral de eliminación de SCL, el agente de filtrado de contenido no elimina el mensaje. En su lugar, compara el valor de nivel de confianza de correo no deseado con el umbral de rechazo de nivel de confianza de correo no deseado.

b) **Umbral de rechazo SCL.** Si el valor de SCL de un mensaje determinado es igual o superior al umbral de rechazo SCL, el agente de filtro de contenido elimina el mensaje y envía una respuesta de rechazo al sistema de envío. Se puede personalizar la respuesta de rechazo y en algunos casos, se envía un informe de no entrega (NDR) al remitente original del mensaje. Si el valor SCL de un mensaje es inferior a los valores de umbral de eliminación y rechazo SCL, el agente de filtrado de contenido no elimina ni rechaza el mensaje. En su lugar, compara el valor del nivel de confianza de correo no deseado con el umbral de cuarentena del nivel de confianza de correo no deseado.

c) **Umbral de cuarentena SCL.** Cuando el valor de SCL de un mensaje determinado es igual o superior al umbral de cuarentena SCL, el agente de filtro de contenido envía el mensaje al buzón de cuarentena. Los administradores de correo electrónico deben revisar periódicamente el buzón de cuarentena. Si el valor SCL de un mensaje es inferior a los valores del umbral de eliminación, rechazo y cuarentena de SCL, el agente de filtrado de contenido no elimina, rechaza ni pone en cuarentena el mensaje. En su lugar, el agente de filtrado de contenido envía el mensaje al servidor de buzones correspondiente, donde se evalúa el valor de umbral de la carpeta correo electrónico no deseado de cada destinatario del mensaje.

d) **Umbral de la carpeta de correo electrónico no deseado.** Si el valor SCL de un mensaje concreto supera el umbral de la carpeta de correo electrónico no deseado, el mensaje se entrega a la carpeta "correo electrónico no deseado" del usuario. Si el valor SCL de un mensaje es inferior a los valores de umbral de eliminación, rechazo, cuarentena y carpeta de correo electrónico no deseado, el mensaje se entrega a la Bandeja de entrada del usuario.

A continuación, se muestran los valores predeterminados de cada umbral, así como el umbral de la carpeta de correo electrónico no deseado configurado a nivel global de organización.



Nota: El agente de filtro de contenido y la carpeta de correo electrónico no deseado procesan el valor de umbral de SCL de manera diferente. El agente de filtro de contenido lleva a cabo una acción según el valor de umbral de SCL que configure. La carpeta de correo electrónico no deseado lleva a cabo una acción según el valor de umbral de SCL que configure más 1. Por ejemplo, si configura la acción "Eliminar" con una SCL de 8 en el agente de filtro de contenido, se eliminarán todos los mensajes con una SCL de 8 o superior. No obstante, si configura la carpeta de correo electrónico no deseado con un valor de umbral de 4, todos los mensajes con una SCL de 5 o superior se pasan a la carpeta de correo electrónico no deseado.

Adicionalmente, el filtro de contenido permite configurar palabras o expresiones personalizadas junto con una acción de permitir o rechazar.

Cuando el agente de filtro de contenido detecta una expresión permitida preconfigurada en un mensaje entrante, dicho agente asigna automáticamente un valor SCL de 0 al mensaje. Por otro lado, cuando detecta una expresión no autorizada configurada en un mensaje entrante, asigna una clasificación SCL de 9.

Una característica interesante, aunque con poca aceptación, es la capacidad del agente de filtro de contenido de realizar validaciones del certificado electrónico de Microsoft Outlook (Outlook Email Postmark validation).

El certificado electrónico Microsoft Outlook es una prueba computacional que Outlook aplica a los mensajes salientes para ayudar a los sistemas de mensajería de los destinatarios a distinguir el correo electrónico legítimo del no deseado y ayuda a reducir la posibilidad de falsos positivos.

Cuando la validación de certificado electrónico Outlook está habilitada, el agente de filtro de contenido analiza el mensaje entrante en busca de un encabezamiento de certificado computacional. La presencia de un encabezamiento de certificado computacional válido y resuelto en el mensaje indica que el equipo del cliente que generó el mensaje resolvió dicho certificado.

Los equipos no necesitan invertir demasiado tiempo en el procesamiento para resolver certificados computacionales individuales. Sin embargo, el procesamiento de certificados de validación de muchos mensajes es inviable para un remitente de correo electrónico no deseado. Hay que recordar que el objetivo fundamental de este tipo de remitentes es enviar la mayor cantidad de mensajes posibles en cortos periodos de tiempo.

Por lo tanto, no es probable que la persona que envía millones de mensajes de correo electrónico no deseado invierta la capacidad de procesamiento necesaria para resolver certificados de todos los correos electrónicos no deseados salientes.

Si el correo electrónico de un remitente contiene un certificado computacional válido y resuelto, no es probable que el remitente sea un remitente malintencionado. En este caso, el agente de filtrado de contenido bajaría la clasificación SCL. Si la característica de validación de certificados está habilitada y un mensaje entrante no contiene un encabezamiento de certificado computacional, o dicho encabezamiento no es válido, el agente de filtro de contenido no variará la clasificación SCL.

Otra funcionalidad que también ayuda a reducir el número de falsos positivos en la detección de correo no deseado es la utilización de las listas de remitentes seguros, de remitentes bloqueados, de destinatarios seguros y de contactos de confianza de Microsoft Outlook.

Esta funcionalidad se denomina "agregación de lista segura" es un conjunto de funcionalidades contra correo no deseado que se comparten entre Outlook y Exchange y es probablemente el método más efectivo para reducir los falsos positivos.

La agregación de lista segura recopila datos de las listas seguras contra correo electrónico no deseado que configuran los usuarios de Outlook y los pone a disposición de los agentes contra correo electrónico no deseado en el servidor Exchange. Posteriormente, el agente de filtro de contenido identifica como seguros los mensajes de correo electrónico que los usuarios de Outlook reciben de los contactos en que han confiado o que han agregado a las listas de destinatarios seguros o de remitentes seguros de Outlook. Así mismo, el agente de filtro de remitentes también realiza un filtrado de remitentes por destinatario mediante el uso de la lista de remitentes bloqueados que configuran los usuarios.

Una recopilación de listas seguras es la combinación de datos de la lista de remitentes seguros, la lista de destinatarios seguros, la lista de remitentes bloqueados y los contactos externos. Estos datos se almacenan en Outlook y en el buzón de Exchange.

Los siguientes tipos de información se almacenan en una recopilación de listas seguras del usuario de Outlook:

a) Remitentes seguros y destinatarios seguros. En el mensaje, el encabezado "De" indica un remitente. El campo "Para" del mensaje de correo electrónico indica un destinatario. Tanto los remitentes seguros como los destinatarios seguros se representan mediante direcciones SMTP completas, como usuario@dominio.com. Los usuarios de Outlook pueden agregar remitentes y destinatarios a sus listas seguras.

b) Remitentes bloqueados. Al igual que hacen con los remitentes seguros, los usuarios pueden bloquear a los remitentes no deseados agregándolos a sus listas de remitentes bloqueados.

c) Dominio seguro. El dominio es la parte de una dirección SMTP que va detrás del símbolo "@". Los usuarios de Outlook pueden agregar dominios remitentes a sus listas seguras.

d) Contactos externos. En la agregación de listas seguras se pueden incluir dos tipos de contactos externos. El primer tipo de contacto externo incluye los contactos a los que los usuarios de Outlook han enviado correo. Esta clase de contacto se agrega a la lista de remitentes seguros únicamente si un usuario de Outlook selecciona la opción correspondiente en la configuración de correo electrónico no deseado de Outlook. El segundo tipo de contacto externo incluye los contactos de Outlook que los usuarios han agregado o importado. Esta clase de contacto se agrega a la lista de remitentes seguros únicamente si un usuario de Outlook selecciona la opción correspondiente en la configuración de filtro de correo electrónico no deseado de Outlook.

Tal y como se ha indicado anteriormente, la colección de listas seguras se almacena en el servidor de buzones de correo del usuario. Un usuario puede tener hasta 1.024 entradas exclusivas en una colección de listas seguras.

Exchange 2016 tiene un asistente de buzón de correo, llamado asistente de buzón de correo para opciones de correo electrónico no deseado, que supervisa los cambios en la colección de listas seguras para los buzones de correo. A continuación, replica esos cambios en Directorio Activo, donde la colección de listas seguras se almacena en cada objeto de usuario.

Cuando la colección de listas seguras se almacena en el objeto de usuario en Directorio Activo, también se agrega a la funcionalidad contra correo electrónico no deseado de Exchange 2016 y se optimiza para minimizar el almacenamiento y la replicación.

Exchange usa los datos almacenados de la colección de listas seguras durante el filtrado de contenido y si existe un servidor de transporte perimetral suscrito en la red perimetral, el servicio Microsoft Exchange EdgeSync replica dicha colección de listas seguras en la instancia Active Directory Lightweight Directory Services (AD LDS) en el servidor de transporte perimetral.

A las entradas de la colección de listas seguras se les aplica un algoritmo hash (SHA-256) unidireccional, antes de almacenarlas como conjuntos de matrices en tres atributos de objeto de usuario, msExchSafeSenderHash, msExchSafeRecipientHash y msExchBlockedSendersHash, como objeto binario de gran tamaño (BLOB).

Al aplicar el algoritmo hash a los datos, se crea una salida de longitud fija, que también es probable que sea única. Para cifrar las entradas de la colección de listas seguras mediante hash, se crea un hash de 4 bytes.

Cuando se recibe un mensaje de Internet, Exchange Server aplica un algoritmo hash a la dirección del remitente y la compara con los algoritmos hash almacenados en nombre del usuario de Outlook al que se envió el mensaje. Si el hash del remitente coincide con el de los remitentes seguros, el mensaje se salta el filtro de contenido. Si el hash del remitente coincide con el de los remitentes bloqueados, el mensaje se bloquea.

El cifrado unidireccional mediante hash de las entradas de la recopilación de listas seguras realiza las siguientes funciones importantes:

a) Reduce el espacio de almacenamiento y replicación. La mayor parte de las veces, la aplicación de hash reduce el tamaño de los datos. Por tanto, para guardar y transmitir una versión cifrada mediante hash de una entrada de la recopilación de listas seguras hace falta menos espacio y el tiempo de replicación se reduce.

b) Genera colecciones de listas seguras que los usuarios malintencionados no pueden usar. Dado que no es posible hacer ingeniería inversa de los valores con hash unidireccional y devolverlos a su dirección SMTP o dominio original, las colecciones de listas seguras no generan direcciones de correo electrónico que los usuarios malintencionados puedan usar y que puedan poner en peligro un servidor de Exchange.

Nota: La agregación de lista segura está habilitada de forma predeterminada en Exchange 2016. A diferencia de versiones anteriores, no es necesario ejecutar manualmente el cmdlet "Update-SafeList" para cifrar con hash y escribir los datos de la colección de listas seguras en Directorio Activo. En Server Exchange 2016, los datos de la colección de listas seguras se escriben en Directorio Activo mediante el asistente de buzón de correo para opciones de correo electrónico no deseado.

6.4.6 AGENTE DE ANÁLISIS DE PROTOCOLO Y REPUTACIÓN DE REMITENTE

La reputación del remitente examina las siguientes estadísticas de mensajes y calcula el nivel de reputación (SRL) correspondiente a cada remitente:

a) **Análisis de comandos HELO/EHLO.** Los comandos SMTP HELO y EHLO están pensados para proporcionar el nombre de dominio o la dirección IP del servidor SMTP remitente al servidor SMTP receptor. Los usuarios malintencionados o spammers suelen falsificar la instrucción HELO/EHLO de diferentes formas como especificar una dirección IP que no coincide con la dirección IP desde la que se originó la conexión o dominios que se admiten de forma local en el servidor de destino para intentar aparentar que los dominios están en la organización. De esta forma, el análisis de la instrucción HELO/EHLO por remitente puede indicar la presencia de un spammer. Por ejemplo, un remitente que proporciona muchas instrucciones HELO/EHLO únicas en un período específico probablemente será un spammer o también es muy probable que sean spammers los remitentes que constantemente proporcionan una dirección IP en la instrucción HELO que no coincide con la dirección IP de origen. También es muy probable que lo sean los remitentes remotos que constantemente proporcionan un nombre de dominio local en la instrucción HELO que está en la misma organización que el servidor de Exchange.

b) **Búsqueda de DNS inversa.** La reputación del remitente también comprueba que la dirección IP de origen desde la que este transmitió el mensaje coincida con el nombre de dominio registrado que envía en el comando SMTP HELO o EHLO. Para ello se lleva a cabo una consulta de DNS inversa enviando la dirección IP de origen al DNS. El resultado que devuelve el DNS debe ser el nombre de dominio registrado mediante el uso de la autoridad de nombres de dominio de esa dirección IP. Posteriormente, se compara el nombre de dominio que devuelve el DNS con el nombre de dominio que el remitente envió en el comando SMTP HELO/EHLO. Si los nombres de dominio no coinciden, es probable que el remitente sea un spammer y que su clasificación general de SRL aumente.

c) **Análisis SCL de los mensajes de un remitente determinado.** Los datos de cada remitente y las clasificaciones que obtienen sus mensajes se guardan para que la reputación del remitente los analice. La reputación del remitente calcula estadísticas para un remitente de acuerdo con la relación entre todos los mensajes de ese remitente que han obtenido una clasificación SCL baja en el pasado y todos los mensajes de ese remitente que han obtenido una clasificación SCL alta en el pasado. Asimismo, a la clasificación SRL general se aplica el número de mensajes con una clasificación SCL alta que ese remitente ha enviado el último día.

d) **Prueba de proxy abierto del remitente.** Un remitente legítimo puede ser un proxy abierto debido a una configuración incorrecta o código dañino, sin embargo, los proxys abiertos constituyen la vía perfecta para que los usuarios malintencionados oculten su identidad verdadera e inicien ataques por denegación de servicio (DoS) o envíen correo no deseado. Además, se pueden usar varios proxys abiertos para ocultar la dirección IP de origen. Si la reputación del remitente realiza una prueba de proxy abierto, lo hace mediante la aplicación de formato a una solicitud SMTP para intentar volver a conectarse al servidor de Exchange desde el proxy abierto. Si se recibe una solicitud SMTP desde el proxy, la reputación del remitente comprueba que el proxy es un proxy abierto y actualiza la estadística de prueba de proxy abierto para ese remitente.

La reputación del remitente compara todas estas estadísticas y calcula un SRL para cada remitente. El SRL es un número comprendido entre el 0 y el 9 que predice la probabilidad de que un remitente específico sea un spammer o usuario malintencionado. El valor 0 indica que probablemente el remitente no sea un spammer, mientras que el valor 9 indica que probablemente lo sea.

Se puede configurar un umbral de bloqueo del 0 al 9, en el que la reputación del remitente emite una solicitud al agente de filtro de remitentes y bloquea al remitente para que no pueda enviar el mensaje a la organización. Cuando se bloquea a un remitente, este se agrega a la lista remitentes bloqueados durante un período configurable.

La forma en la que se tratan los mensajes depende de la configuración del agente de filtro de remitentes. Las siguientes acciones son las que se pueden elegir para tratar los mensajes bloqueados:

a) Rechazar.

b) Eliminar.

c) Aceptar y marcar como remitente bloqueado.

Si el remitente está incluido en la lista de bloqueo de IP o servicio de reputación de IP de Microsoft, el agente de reputación de remitente emite una solicitud inmediata al agente de filtro del remitente para bloquear al remitente. Para aprovechar esta funcionalidad, se debe habilitar y configurar el servicio de actualización contra correo no deseado de Microsoft Exchange.

Así mismo, de forma predeterminada, el servidor de transporte perimetral establece una clasificación de 0 para los remitentes que no se han analizado. Cuando un remitente ha enviado 20 o más mensajes, la reputación del remitente calcula un SRL basado en las estadísticas descritas anteriormente.

6.4.7 AGENTE DE FILTRO DE DATOS ADJUNTOS

El filtro de datos adjuntos permite aplicar filtros para controlar los datos adjuntos que reciben los usuarios. El filtro de datos adjuntos es cada vez más importante en los entornos actuales, en los que muchos de estos documentos contienen virus dañinos o material inadecuado que pueden causar daños importantes en el equipo del usuario o en toda la organización, provocando daños en documentación importante o haciendo pública información confidencial.

Los siguientes tipos de filtro de datos adjuntos están disponibles en Exchange Server 2016 para controlar los datos adjuntos que entran o salen de la organización:

a) **Filtrado basado en el nombre o la extensión del archivo.** Se pueden filtrar los datos adjuntos especificando el nombre de archivo exacto o la extensión que se deberá filtrar. Un ejemplo de nombre de archivo exacto es "NombredeArchivoMalo.exe". Un ejemplo de extensión del archivo es "*.exe".

b) **Filtrado basado en el tipo de contenido MIME del archivo.** También se pueden filtrar los datos adjuntos especificando el tipo de contenido MIME que se filtrará. Los tipos de contenido MIME indican el tipo de datos adjuntos; si es una imagen JPEG, un archivo ejecutable, un archivo Microsoft Office Excel u otro tipo de archivo. Los tipos de contenido se expresan como "type/subtype". El tipo de contenido de imagen JPEG se expresa como "image/jpeg".

Si los datos adjuntos coinciden con uno de estos criterios de filtrado, se puede configurar una de las siguientes acciones para llevarla a cabo con los datos adjuntos.

a) Rechazar. Si la configuración de acciones está establecida en rechazar, no se entregará el mensaje de correo electrónico ni el documento adjunto al destinatario, y el sistema generará un mensaje de error de notificación de estado de envío (DSN) para el remitente. Se puede personalizar la respuesta de rechazo.

b) Eliminación silenciosa. Si la configuración de acciones está establecida en eliminación silenciosa, no se entregará ni el mensaje de correo electrónico ni el documento adjunto al destinatario. Tampoco se notifica al remitente que se han bloqueado el mensaje de correo electrónico y el documento adjunto.

c) Seccionar. Si la configuración de acciones está establecida en seccionar, el documento adjunto se quitará del mensaje de correo electrónico. Este valor permite que se entreguen al destinatario el mensaje y otros documentos adjuntos que no coinciden con ninguna entrada de la lista de bloqueo de documentos adjuntos. Además, se agregará una notificación de que el documento adjunto está bloqueado al mensaje de correo electrónico del destinatario.

Nota: Es importante señalar que el agente de filtro de datos adjuntos que se incluye con Exchange Server 2016 detecta los tipos de archivos incluso si se les ha cambiado el nombre. El filtrado de datos adjunto comprueba además que los archivos Zip y LZH comprimidos no contengan datos adjuntos bloqueados mediante una comparación de las extensiones de nombre de archivo con los archivos del archivo Zip o LZH comprimido. Sin embargo, el filtro de datos adjuntos sólo está disponible en el servidor perimetral de Exchange Server 2016.

Aunque, como se ha indicado, el filtro de datos adjuntos sólo está disponible cuando se implementa un servidor de transporte perimetral de Exchange Server 2016, si su organización sólo dispone del servidor de buzones, tal y como se plantea en esta guía, se pueden aprovechar las reglas de transporte para realizar una gestión de datos adjuntos bajo ciertas condiciones como las siguientes:

a) Búsqueda de archivos en datos adjuntos comprimidos, tales como ".zip" y ".rar".

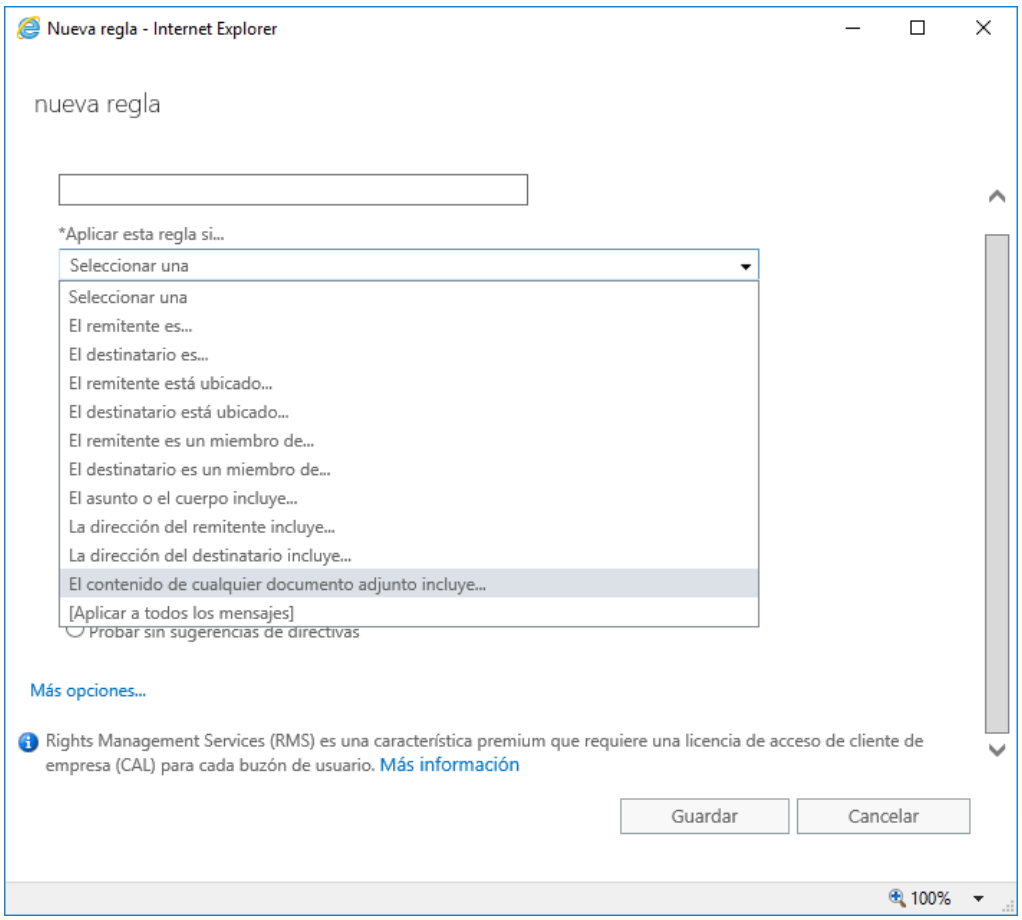
b) Inspección del contenido de los datos adjuntos en busca de palabras clave especificadas.

c) Inspección de los datos adjuntos en busca de contenido ejecutable.

d) Comprobación de los mensajes con datos adjuntos que no se puede inspeccionar y, a continuación, impedir que se envíe el mensaje completo.

e) Comprobación de los datos adjuntos que superen un determinado tamaño.

f) Bloqueo de todos los mensajes que contengan datos adjuntos.



6.4.8 ANÁLISIS FRENTE A CÓDIGO DAÑINO

Exchange Server 2016 incluye un motor frente a código dañino integrado en el servidor de buzones. Se trata, sin embargo, de una protección básica frente código dañino, la cual puede desactivarse, sustituirse, o emparejarse con un servicio basado en la nube (como Microsoft Exchange Online Protection) para proporcionar mejores niveles de defensa.

Nota: Los administradores de Microsoft Exchange Server 2016 pueden descargar manualmente las actualizaciones del motor frente a código dañino y de la firma de definiciones. Se recomienda descargar dichas actualizaciones en su servidor de Exchange antes de empezar a utilizarlo en producción. Así mismo, para escenarios de alta seguridad donde los servidores no disponen de conexión con Internet, se pueden descargar las actualizaciones de código dañino en modo offline mediante el script disponible en https://support.microsoft.com/es-es/kb/2292741. La descarga se puede realizar desde cualquier PC con conexión a internet y posteriormente copiar el contenido a los servidores Exchange.

Para descargar manualmente las actualizaciones del motor frente código dañino desde una ubicación alternativa, puede ejecutar el siguiente comando desde el Shell de administración de Exchange.

```
& $env:ExchangeInstallPath\Scripts\Update-MalwareFilteringServer.ps1 -Identity <Nombre FQDN del servidor>  -EngineUpdatePath \\Servidor\share
```

Posteriormente, en el visor de eventos del sistema se registrarán una serie de entradas con origen FIPFS indicando el resultado de la actualización manual.

Durante el proceso de instalación de Exchange Server, se solicita si se mantiene habilitado el análisis de código dañino o se deshabilita. En caso de mantener el análisis de código dañino habilitado, se crea una directiva predeterminada.

La directiva frente a código dañino predeterminada controla la configuración de filtrado de código dañino de toda la organización Exchange. Los administradores pueden ver y editar, aunque no eliminar, la directiva frente a código dañino predeterminada para que se adapte mejor a las necesidades de la organización.

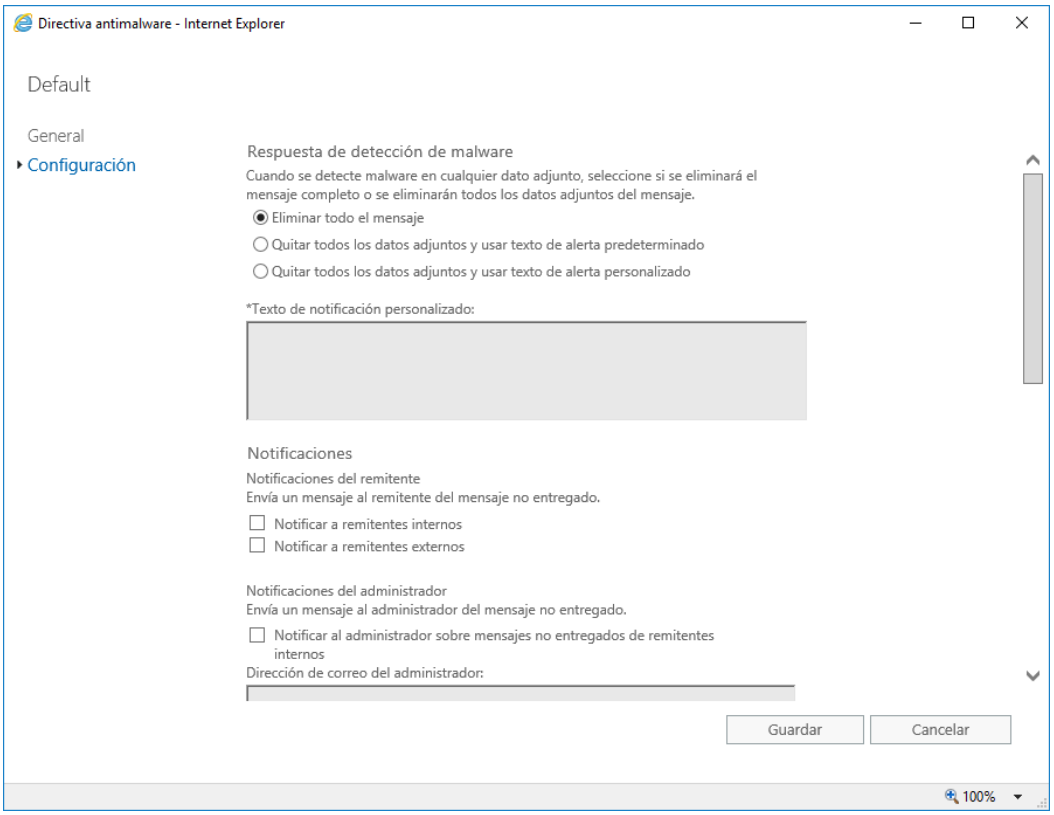
También se puede crear directivas personalizadas de filtro de código dañino y aplicarlas a usuarios, grupos o dominios específicos de la organización. Las directivas personalizadas siempre tienen prioridad con respecto a la directiva predeterminada, sin embargo, se puede cambiar la prioridad de ejecución de las directivas personalizadas.

La configuración de la directiva predeterminada de análisis de código dañino elimina todo el mensaje si se detecta que contiene algún tipo de código dañino. No notifica la eliminación ni al remitente, ni al destinatario. Esta configuración se puede editar, con las opciones:

a) Eliminar todo el mensaje.

b) Quitar todos los datos adjuntos y usar texto de alerta predeterminado.

c) Quitar todos los datos adjuntos y usar texto de alerta personalizado.



6.4.9 FILTRO DE CORREO ELECTRÓNICO NO DESEADO DE OUTLOOK

Una vez que se ha aplicado todos los filtros y se ha explorado el mensaje en busca de virus, el mensaje se envía al buzón del destinatario deseado y se aplica el filtrado de correo electrónico no deseado.

Si la clasificación de SCL para el mensaje es mayor o igual al umbral de la carpeta de correo electrónico no deseado de SCL y este umbral está activado, el servidor del buzón colocará el mensaje en la carpeta de correo electrónico no deseado del usuario de Outlook. Si el valor de SCL de un mensaje es inferior a los valores de umbral de eliminación, rechazo, cuarentena y de carpeta de correo electrónico no deseado, entonces el servidor del buzón colocará el mensaje en la bandeja de entrada del usuario.

6.5 CUARENTENA DE EXCHANGE SERVER 2016

Muchas organizaciones están obligadas por leyes o normativas a conservar o hacer entrega de todos los mensajes de correo electrónico legítimos.

La cuarentena de correo no deseado es una característica del agente de filtro de contenido que reduce el riesgo de perder dichos mensajes legítimos. Para ello, se proporciona una ubicación de almacenamiento temporal para aquellos mensajes identificados como correo no deseado que no deben ser entregados a un buzón de usuario dentro de la organización, pero que tampoco se deben perder.

Los mensajes identificados por el agente de filtro de contenido como correo no deseado se envuelven en un informe de no entrega (NDR) y se entregan a un buzón específico de cuarentena de correo no deseado dentro de la organización.

Posteriormente, los administradores o responsables de cuarentena pueden administrar los mensajes entregados al buzón de cuarentena y tomar las medidas pertinentes como eliminar mensajes o dejar que los mensajes marcados como falsos positivos en el filtrado contra correo no deseado se enruten hacia los destinatarios a los que iban dirigidos.

Además, se puede configurar el buzón de cuarentena de correo no deseado de forma que los mensajes se eliminen automáticamente después de un periodo determinado de tiempo.

Además, la cuarentena se puede utilizar para ajustar los diferentes umbrales de correo electrónico no deseado y reducir el número de falsos positivos que se pudieran originar. Para ello, es muy importante saber interpretar las marcas de correo no deseado que incluye Exchange Server 2016 en todos los mensajes que han sido analizados.

6.5.1 MARCAS DE CORREO NO DESEADO

Las marcas de correo electrónico no deseado ayudan a diagnosticar los problemas relacionados con el correo no deseado mediante la aplicación de metadatos de diagnóstico, o marcas, como información específica del remitente, resultados de la validación del puzle y resultados del filtrado de contenido, a los mensajes, mientras pasan a través de las características contra correo electrónico no deseado que filtran los mensajes entrantes de Internet.

Hay cuatro marcas contra correo electrónico no deseado:

a) La marca de nivel de confianza contra suplantación de identidad (phishing).

b) La marca de nivel de confianza contra correo no deseado.

c) La marca de identificación de remitente.

d) La marca de informe contra correo no deseado.

Se puede usar las marcas de correo electrónico no deseado como herramientas de diagnóstico para determinar las acciones que se deben realizar con los falsos positivos y los mensajes que se sospecha que son correo electrónico no deseado que reciben las personas en los buzones.

Las marcas de correo electrónico no deseado se pueden ver mediante Microsoft Outlook, abriendo los encabezados del mensaje original, desde las propiedades del propio mensaje.

A continuación, se muestra un ejemplo de informe de diagnóstico de correo electrónico no deseado con las diferentes marcas registradas:

```
–X-MS-Exchange-Organization-Antispam-Report: DV:<DATVersion>;CW:CustomList; PCL:
PhishingVerdict <verdict>;P100:PhishingBlock;PP:Presolve;SID: SenderIDStatus <status>;TIME:
<SendReceiveDelta>;MIME:MimeCompliance
```

La siguiente tabla muestra la información de filtrado incluida en un informe de correo electrónico no deseado.

Marca	Descripción
SID	La marca de Identificación del remitente (SID) se basa en la estructura de directivas del remitente (SPF) que autoriza el uso de dominios en el correo electrónico. El encabezado SPF aparece en el sobre del mensaje como Received-SPF. El proceso de evaluación puede devolver con uno de los valores siguientes: – **Pass.** La dirección IP y la Dirección responsable pretendida (PRA) han superado la comprobación del Id. de remitente. – **Neutral.** Los datos del Id. de remitente publicados no son explícitamente concluyentes. – **Soft fail.** Es posible que la dirección IP de la PRA no esté en el conjunto permitido. – **Fail.** La dirección IP no está permitida; no se encontró ninguna PRA en el correo entrante o no existe el dominio remitente. – **None.** No hay datos publicados de la SPF en el DNS del remitente. – **TempError.** Ha ocurrido un error temporal de DNS como, por ejemplo, un servidor DNS no disponible. – **PermError.** El registro DNS no es válido; por ejemplo, existe un error en el formato de registro. Además, la marca de Identificación del remitente aparece como un encabezado X en el sobre del mensaje, tal y como se indica a continuación: X-MS-Exchange-Organization-SenderIdResult:<estado>
DV	La marca de versión del DAT (DV) indica la versión del archivo de definición de correo electrónico no deseado que se utilizó al examinar el mensaje.
SA	La marca de acción de firma (SA) indica que el mensaje se ha recuperado o se ha eliminado porque se ha encontrado una firma en el mensaje.
SV	La marca de versión del DAT de firma (SV) indica la versión del archivo de firma que se utilizó al examinar el mensaje.
PCL	La marca de nivel de confianza de suplantación de identidad (phishing) (PCL) muestra la calificación del mensaje en función de su contenido y se aplica cuando el agente de filtrado de contenido procesa el mensaje. Este estado se puede devolver con uno de los valores siguientes: – **Neutral.** No es probable que el contenido del mensaje sea suplantación de identidad (phishing). – **Suspicious.** Es probable que el contenido del mensaje sea phishing. El valor de PCL varía de 1 a 8. Una calificación de PCL de 1 a 3 devuelve el estado de Neutral. Esto significa que no es probable que el contenido del mensaje sea suplantación de identidad (phishing). Una calificación de PCL de 4 a 8 devuelve un estado de Suspicious. Esto significa que es probable que el mensaje sea "phishing". Estos valores se utilizan para determinar qué medidas toma Outlook con los mensajes. Outlook usa la marca PCK para bloquear el contenido de los mensajes sospechosos. La marca PCL aparece como una cabecera X en el sobre del mensaje, tal y como se indica a continuación: X-MS-Exchange-Organization-PCL:<estado>

Marca	Descripción
SCL	La marca del nivel de confianza de correo no deseado (SCL) del mensaje muestra la calificación del mensaje en función de su contenido. El agente de filtrado de contenido usa la tecnología SmartScreen de Microsoft para evaluar el contenido de un mensaje y asignar una clasificación de confianza de correo no deseado para cada mensaje. El valor de SCL se encuentra de 0 a 9, donde 0 indica que es poco probable que sea correo electrónico no deseado y 9 indica que es más probable que sea correo electrónico no deseado. Las acciones que Exchange y Outlook realizan dependen de la configuración de los umbrales de SCL. La marca SCL aparece como una cabecera X en el sobre del mensaje, tal y como se indica a continuación: X-MS-Exchange-Organization-SCL:<estado>
CW	La marca de ponderación personalizada (CW) de un mensaje indica que el mensaje contiene una palabra o una frase no aprobada y que el valor de SCL, o ponderación de esa palabra o frase no aprobada se ha aplicado a la calificación final de SCL: Las frases no aprobadas, o frases no admitidas, tienen una ponderación máxima y cambian la calificación de SCL a 9. Las palabras o frases aprobadas, o frases admitidas, tienen una ponderación mínima y cambian la calificación de SCL a 0.
PP	La marca del puzle resuelto previamente (PP) indica que, si un mensaje del remitente contiene un certificado electrónico válido y resuelto, basado en la funcionalidad de validación del certificado electrónico de Outlook, no es probable que se trate de un remitente malintencionado. En este caso, el agente Filtro de contenido reduciría la calificación de SCL. El agente de filtrado de contenido no cambia la calificación de SCL si la característica de validación de certificado electrónico está habilitada y si se cumple alguna de las siguientes condiciones: – Un mensaje entrante no contiene un encabezado de certificado electrónico. – El encabezado del certificado electrónico no es válido.
TIME:Time Based Features	La marca TIME indica que hay un tiempo de retraso importante entre la hora a la que se envió el mensaje y la hora a la que se recibió. La marca TIME se usa para determinar la calificación SCL final del mensaje.
MIME: MIME Compliance	La marca MIME indica que el mensaje de correo electrónico no es compatible con MIME.
P100:Phishing Block	La marca P100 indica que el mensaje contiene una dirección URL que está presente en un archivo de definición de suplantación de identidad (phishing).
IPOnAllowList	La marca IPOnAllowList indica que la dirección IP del remitente se encuentra en la lista de IP permitidas.
Message Security Antispam Bypass	La marca MessageSecurityAntispamBypass indica que no se ha filtrado el contenido del mensaje y que se ha concedido al remitente permiso para eludir los filtros contra correo electrónico no deseado.
Sender Bypassed	La marca SenderBypassed indica que el agente de filtrado de contenido no procesa el filtrado de contenido de los mensajes recibidos de este remitente.

Marca	Descripción
AllRecipients Bypassed	La marca AllRecipientsBypassed indica que se ha cumplido una de las condiciones siguientes para todos los destinatarios incluidos en el mensaje: – El parámetro AntispamBypassedEnabled del buzón de correo del destinatario está establecido en $true. Esta es una configuración para destinatarios que sólo puede establecer un administrador con el cmdlet Set-Mailbox. – El remitente del mensaje se encuentra en la lista de remitentes seguros de Outlook del destinatario.

6.6 CUENTA ADMINISTRATIVA DE INSTALACIÓN

La cuenta administrativa de instalación se utiliza para instalar y configurar cada servidor dentro de la organización de servidores de Exchange Server 2016.

El proceso de instalación de Exchange Server 2016 incluye varias fases dependiendo de si se trata de la instalación del primer servidor de la organización, servidores adicionales o si se está realizando una migración desde versiones anteriores.

Antes de instalar Microsoft Exchange Server 2016, debe prepararse el bosque de Active Directory y sus dominios correspondientes.

El primer paso al preparar una organización para Exchange 2016 es extender el esquema de Active Directory. Exchange almacena mucha información en Active Directory, pero para poder hacerlo deben agregarse y actualizarse clases, atributos y otros elementos.

Antes de extender el esquema, es importante tener en cuenta lo siguiente:

a) La cuenta con la que inicie sesión debe ser miembro de los grupos de seguridad administradores de esquema y administradores de empresa.

b) El equipo donde ejecute el comando para ampliar el esquema debe encontrarse en el mismo sitio y el mismo dominio de Directorio Activo que el maestro de esquema.

c) Si usa el parámetro "DomainController", asegúrese de especificar el nombre del controlador de dominio que actúa como maestro de esquema.

PrepareSchema. Este paso en el proceso de instalación conecta con el maestro de esquema e importa los archivos del formato de intercambio de datos del protocolo LDAP (LDIF) para actualizar el esquema del Directorio Activo con los atributos específicos de Exchange Server 2016. Los archivos LDIF se copian en el directorio temporal y, una vez se han importado al esquema, se eliminan. Solo es necesario ejecutar este paso una vez en cada bosque donde se vaya a instalar Exchange Server 2016. Para extender el esquema, se debe ejecutar el comando:

```
Setup.exe /PrepareSchema /IAcceptExchangeServerLicenseTerms
```

Una vez extendido el esquema de Active Directory, ya se puede preparar otros elementos de Directorio Activo para Exchange 2016. Durante el siguiente paso, Exchange crea contenedores, objetos y otros elementos de Directorio Activo donde se almacenará la información.

La colección de todos los contenedores, objetos y atributos de Exchange se conoce como organización de Exchange.

Antes de preparar Active Directory para Exchange, es importante tener en cuenta lo siguiente:

a) La cuenta con la que inicie sesión debe ser miembro del grupo de seguridad Administradores de empresa. Si ha omitido el paso 1 para que el comando PrepareAD extienda el esquema, la cuenta que use también debe ser miembro del grupo de seguridad Administradores de esquema.

b) El equipo donde ejecute el comando debe encontrarse en el mismo sitio y el mismo dominio de Active Directory que el maestro de esquema. También deberá ponerse en contacto con todos los dominios del bosque en el puerto TCP 389.

Al ejecutar el comando de preparación del dominio de Directorio Activo, se necesitará asignar un nombre a la organización de Exchange. Este nombre se usa de forma interna en Exchange y, por lo general, resulta visible para los usuarios. Es frecuente usar como nombre de organización el nombre de la compañía donde se está instalando Exchange. El nombre que use no afectará a la funcionalidad de Exchange ni determinará qué puede usar o no para las direcciones de correo electrónico.

PrepareAD. Como ya se ha indicado, este paso en el proceso de instalación crea el contenedor Microsoft Exchange en el dominio de Directorio Activo correspondiente. Además, comprueba que se ha actualizado el esquema y crea toda la estructura de contenedores, objetos y grupos de seguridad necesarios para la instalación de los servidores Exchange. Para preparar el dominio actual se debe ejecutar el siguiente comando:

```
Setup.exe /PrepareAD /OrganizationName:"<NOMBRE>" /IAcceptExchangeServerLicenseTerms
```

Así mismo, se debe ejecutar en cada dominio del bosque donde existan servidores de Exchange 2016, objetos habilitados para correo o servidores de catálogo global que es posible que usen los componentes de acceso a directorios de Exchange.

Para preparar todos los dominios de Directorio Activo, se puede utilizar el parámetro PrepareAllDomains al ejecutar el programa de instalación. El programa preparará todos los dominios para Exchange en el bosque de Active Directory. En este caso el comando a ejecutar es:

```
Setup.exe /PrepareAllDomains /IAcceptExchangeServerLicenseTerms
```

Si, por el contrario, se requiere elegir qué dominios de Directorio Activo se van a preparar, se puede utilizar el parámetro PrepareDomain al ejecutar el programa de instalación. Si usa el parámetro PrepareDomain, es necesario incluir el nombre de dominio completo (FQDN) del dominio que se desee preparar:

```
Setup.exe /PrepareDomain:<FQDN> /IAcceptExchangeServerLicenseTerms
```

Nota: Puede analizar en detalle los cambios en el esquema de Directorio Activo que se producen durante la instalación de Exchange Server 2016 en el paso "PrepareSchema" en la página Web de Microsoft Technet: https://docs.microsoft.com/es-es/exchange/plan-and-deploy/active-directory/ad-changes?view=exchserver-2016

6.7 PERMISOS

Microsoft Exchange Server 2016, al igual que sus predecesores Exchange Server 2013 y 2010, incluye una amplia variedad de permisos predefinidos, basados en el modelo de permisos control de acceso basado en roles (RBAC), el cual se puede usar desde el primer momento para conceder de forma fácil permisos a los administradores de la organización y a los propios usuarios.

Se pueden usar las características de permisos de Exchange Server 2016 para preparar y poner en marcha la nueva organización de forma rápida y ágil. Así mismo, RBAC concede los permisos necesarios para administrar adecuadamente los roles de servidor Buzón de correo y Acceso de clientes.

En Exchange Server 2016, 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.

Existen dos tipos de roles, los roles administrativos y los roles de usuario final:

a) **Roles administrativos.** Estos roles contienen permisos que se pueden asignar a los administradores o usuarios especialistas mediante grupos de roles que administran una parte de la organización de Exchange, como destinatarios, servidores o bases de datos.

b) **Roles de usuario final.** Estos roles, asignados mediante directivas de asignación de roles, permiten a los usuarios administrar aspectos de su propio buzón de correo y de los grupos de distribución de que disponen. Los roles de usuario final empiezan por el prefijo "My".

Exchange Server 2016 incluye de forma predetermina más de 80 funciones de administración integrados y preconfigurados para su utilización inmediata. A continuación, se muestra una lista con los roles de administración integrados. Puede encontrar más información de cada uno de estos roles en la siguiente página Web:

https://docs.microsoft.com/es-es/exchange/permissions/permissions?view=exchserver-2016

Roles de administración integrados	
Rol Permisos de Active Directory	Rol MyDiagnostics
Rol Listas de direcciones	Rol MyDisplayName
Rol ApplicationImpersonation	Rol MyDistributionGroupMembership
Rol ArchiveApplication	Rol MyDistributionGroups
Rol Registros de auditoría	Rol MyMobileInformation
Rol Agentes de extensión de cmdlet	Rol MyName
Rol Prevención de pérdida de datos	Rol MyPersonalInformation
Rol Grupos de disponibilidad de base de datos	Rol MyProfileInformation
Rol Copias de base de datos	Rol MyRetentionPolicies
Rol Bases de datos	Rol MyTeamMailboxes
Rol Recuperación ante desastres	Rol MyTextMessaging
Rol de grupos de distribución	Rol MyVoiceMail
Rol Suscripciones perimetrales	Rol OfficeExtensionApplication

Roles de administración integrados	
Rol Directivas de dirección de correo electrónico	Rol Aplicaciones personalizadas de la organización
Rol Conectores de Exchange	Rol de aplicaciones del mercado de la organización
Rol Certificados del servidor de Exchange	Rol Acceso de clientes de la organización
Rol Servidores de Exchange	Rol Configuración de la organización
Rol Directorios virtuales de Exchange	Rol Configuración de transporte de la organización
Rol Uso compartido federado	Rol Protocolos POP3 e IMAP4
Rol Administración de derechos de información	Rol Carpetas públicas
Rol Registro en diario	Rol Conectores de recepción
Rol Retención legal	Rol Directivas de destinatarios
Rol LegalHoldApplication	Rol Dominios remotos y aceptados
Rol Carpetas públicas habilitadas para correo	Rol Restablecer contraseña
Rol Creación de destinatarios de correo	Rol Administración de la retención
Rol Destinatarios de correo	Rol Administración de roles
Rol Sugerencias para correo electrónico	Rol Pertenencia y Creación de grupos de seguridad
Rol Importar/Exportar buzón	Rol Conectores de envío
Rol Búsqueda entre buzones	Rol Diagnósticos de soporte
Rol MailboxSearchApplication	Rol Buzones de equipo
Rol Seguimiento de mensajes	Rol TeamMailboxLifecycleApplication
Rol de migración	Rol Agentes de transporte
Rol Supervisión	Rol Higiene de transporte
Rol Mover buzones	Rol Colas de transporte
Rol Mis aplicaciones personalizadas	Rol Reglas de transporte
Rol My Marketplace Apps	Rol Buzones de mensajería unificada
Rol MyAddressInformation	Rol Mensajes de mensajería unificada
Rol MyBaseOptions	Rol Mensajería unificada
Rol MyContactInformation	Rol Administración de roles sin ámbito
Rol Configuración con permiso de vista	Rol Opciones de usuario
Rol Destinatarios con permiso de vista	Rol UserApplication
Rol Registros de auditoría con permiso de vista	

Los roles conceden a los administradores y usuarios permisos para realizar tareas poniendo cmdlets a disposición de aquellos usuarios que tienen asignados los roles en cuestión. Puesto que la consola de administración de Exchange (EAC) y el Shell de administración de Exchange usan cmdlets de PowerShell, al conceder acceso a un cmdlet, el administrador o usuario tiene permiso para realizar la tarea en cada una de las interfaces de administración de Exchange.

La principal ventaja de este modelo es que con RBAC no es necesario modificar ni administrar las listas de control de acceso, como sucedía en Exchange Server 2007. Las listas de control de acceso dificultaban el uso de Exchange 2007, pues había que modificarlas sin causar resultados no deseados, había que mantener dichas modificaciones en las actualizaciones posteriores y había que solucionar los problemas que pudieran surgir al no utilizarlas de la forma habitual.

RBAC permite controlar lo que los administradores y los usuarios finales pueden hacer, ya sea de un modo general o pormenorizado, así como alinear más exactamente los roles que se asignan a usuarios y administradores con los verdaderos roles que éstos desempeñan dentro de la organización.

En Exchange 2007, el modelo de permisos de servidor se aplicaba solamente a los administradores encargados de la infraestructura de Exchange 2007. Sin embargo, en Exchange Server 2016 se controlan tanto las tareas administrativas que se pueden llevar a cabo como las posibilidades que tienen los usuarios de administrar su propio buzón y grupos de distribución.

Así mismo, mediante RBAC se pueden asignar permisos a los usuarios de una organización de dos formas distintas: en función de si el usuario es administrador o usuario experto, o bien usuario final, además de por grupos de roles de administración o directivas de asignación de roles de administración. Cada método asocia a los usuarios con los permisos que necesitan para realizar su trabajo. También se puede usar un tercer método más avanzado, la asignación directa de roles de usuario.

6.7.1 GRUPOS DE FUNCIONES DE ADMINISTRACIÓN

Un grupo de roles de administración es un grupo de seguridad universal (USG) usado en el modelo de permisos de Control de acceso basado en roles (RBAC) en Microsoft Exchange Server 2016.

Los grupos de roles de administración simplifican la asignación de roles de administración a un grupo de usuarios ya que, a todos los miembros de un grupo de funciones se les asigna el mismo conjunto de funciones.

Por otro lado, los grupos de funciones son funciones de administrador y de especialistas asignadas que definen las tareas administrativas principales de Exchange 2016, tales como la administración de la organización, la administración de destinatarios y otras tareas. Los grupos de funciones permiten asignar fácilmente un conjunto de permisos más amplio a un grupo de administradores o usuarios especialistas.

Los grupos de funciones normalmente están relacionados con funciones de administración pública que permiten que los administradores y los usuarios especialistas administren la configuración de su organización y destinatarios. Por ejemplo, con los grupos de funciones se controla si los administradores pueden administrar a los destinatarios o utilizar características de detección de buzones.

La forma más común de asignar permisos a administradores o usuarios especialistas consiste en agregar usuarios a los grupos de roles o quitarlos.

Los grupos de roles constan de los siguientes componentes, que definen lo que los administradores y usuarios especialistas pueden llevar a cabo:

a) Grupo de roles de administración. El grupo de roles de administración es un grupo de seguridad universal especial que contiene buzones, usuarios, grupos de seguridad universal y otros grupos de roles que son miembros del grupo en cuestión. Aquí es donde se agregan y quitan miembros, y también adonde se asignan los roles de administración. La combinación de todos los roles de un grupo de roles define todo lo que los usuarios agregaron a un grupo de roles de la organización Exchange.

b) Rol de administración. Un rol de administración es un contenedor para una agrupación de entradas de roles de administración. Los roles se usan para definir las tareas específicas que pueden realizar los miembros de un grupo de roles asignados a un rol. Una entrada de rol de administración es un cmdlet, un script o un permiso especial que permite realizar todas y cada una de las tareas que tiene un rol.

c) Asignación de roles de administración. Una asignación de roles de administración vincula un rol con un grupo de roles. La asignación de un rol a un grupo de roles permite que los miembros de dicho grupo usen los cmdlets y los parámetros definidos en el rol. Las asignaciones de roles pueden usar ámbitos de administración para controlar dónde se puede usar la asignación.

d) Ámbito de roles de administración. Un ámbito de roles de administración es el ámbito de influencia o de impacto sobre una asignación de roles. Cuando un rol se asigna con un ámbito a un grupo de roles, el ámbito de administración define qué objetos puede administrar esa asignación. A continuación, los miembros del grupo de roles reciben la asignación y su ámbito, los cuales restringen lo que estos miembros pueden administrar. Un ámbito puede estar formado por una lista de servidores o bases de datos, unidades organizativas o filtros en servidores, bases de datos u objetos de destinatario.

Al agregar un usuario a un grupo de roles, el usuario obtiene todos los roles que dicho grupo tiene asignados. Si hay ámbitos aplicados a cualquier asignación de roles entre el grupo de roles y los roles, dichos ámbitos establecerán la configuración de servidor o los destinatarios que el usuario podrá administrar.

En caso de que desee cambiar los roles que se han asignado a los grupos de roles, se deberá cambiar las asignaciones que vinculan los grupos con los roles. De todas formas, no será necesario modificar dichas asignaciones a menos que las creadas en Exchange Server 2016 no se ajusten a sus necesidades.

Las siguientes son las capas que constituyen el modelo de grupo de funciones:

a) Poseedor de función. Un poseedor de función es un buzón que se puede agregar como miembro de un grupo de funciones. Cuando el buzón se agrega como miembro de un grupo de funciones, las asignaciones que se realizaron entre las funciones de administración y un grupo de funciones se aplican al buzón. Esto otorga al buzón todos los permisos proporcionados por las funciones de administración.

b) Grupo de funciones de administración. El grupo de funciones de administración es un grupo de seguridad universal especial que contiene buzones miembros del grupo de funciones. Aquí es donde agrega o quita miembros y, además, a donde se asignan las funciones de administración. La combinación de todas las funciones de un grupo de funciones define todo lo que los usuarios agregaron a un grupo de funciones en la organización Exchange.

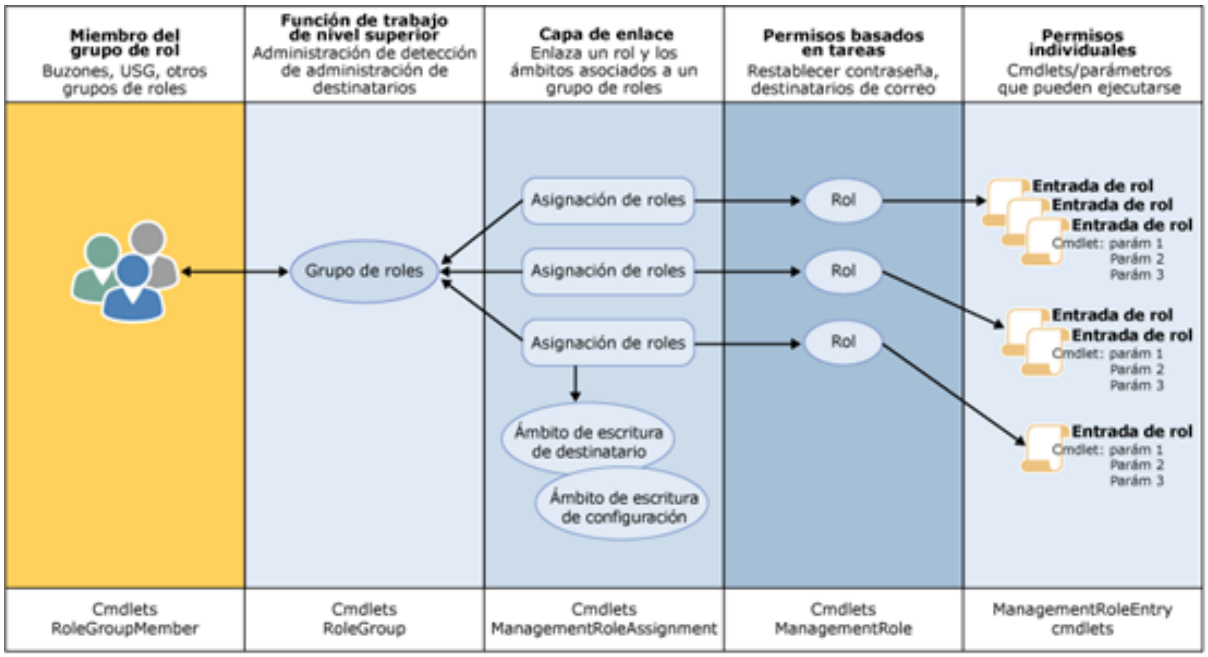
c) Asignación de funciones de administración. Una asignación de funciones de administración vincula una función de administración con un grupo de funciones. La asignación de funciones de administración para un grupo de funciones permite que los miembros del grupo de funciones usen los cmdlets y los parámetros definidos en la función de administración. Las asignaciones de funciones pueden usar ámbitos de administración para controlar dónde se puede usar la asignación.

d) Ámbito de funciones de administración. Un ámbito de funciones de administración es el ámbito de influencia o de impacto en una asignación de funciones. Cuando una función se asigna con un ámbito a un grupo de funciones, el ámbito de administración define qué objetos puede administrar esa asignación. La asignación y su ámbito se otorgan luego a los miembros del grupo de funciones, lo cual restringe lo que pueden administrar esos miembros. Un ámbito puede estar formado por listas de servidores o bases de datos, unidades organizativas o filtros en los objetos del servidor, la base de datos o los destinatarios.

e) Función de administración. Una función de administración es un contenedor para una agrupación de entradas de funciones de administración. Las funciones se usan para definir las tareas específicas que pueden realizar los miembros de un grupo de funciones asignados a una función.

f) Entradas de funciones de administración. Las entradas de funciones de administración son las entradas individuales de una función de administración que brindan acceso a los cmdlets, scripts y otros permisos especiales que dan acceso para realizar una tarea específica. La mayoría de las veces, las entradas de funciones constan de un solo cmdlet y de los parámetros a los cuales se puede tener acceso mediante la función de administración y, por lo tanto, el grupo de funciones al cual la función es asignada.

La siguiente figura, procedente de Microsoft Technet, muestra cada una de las capas del grupo de funciones de la lista precedente y cómo, todas ellas se relacionan entre sí.



Los grupos de funciones integrados son funciones que se incluyen con Exchange 2016 y que proporcionan un conjunto de funciones que se pueden utilizar desde el primer momento para ofrecer niveles variados de permisos administrativos a los grupos de usuarios.

Se pueden agregar usuarios a cualquier grupo de funciones integrado o quitarlos de ellos. Además, se pueden agregar las asignaciones de funciones a la mayoría de los grupos de funciones o quitarlas de ellos. Las únicas excepciones son las siguientes:

a) No se puede quitar ninguna asignación de funciones de delegación del grupo de funciones "Administración de la organización".

b) No se puede quitar la función de administración de funciones del grupo de funciones "Administración de la organización".

La siguiente tabla enumera todos los grupos de funciones integrados incluidos en Exchange Server 2016.

Grupo de funciones integradas	Descripción
Administración de organizaciones	Los administradores que son miembro del grupo de funciones "Administración de la organización" tienen acceso administrativo a toda la organización de Exchange 2016 y pueden realizar casi todas las tareas de administración en cualquier objeto de Exchange 2016, con algunas excepciones, como la función o rol "Discovery Management".
Administración de organizaciones con permiso de vista	Los administradores que son miembros del grupo de funciones "Administración de la organización" de solo visualización pueden ver las propiedades de todos los objetos de la organización de Exchange.
Administración de destinatarios	Los administradores miembros del grupo de funciones "Administración de destinatarios" tienen acceso administrativo para crear o modificar destinatarios de Exchange 2016 dentro de la organización de Exchange 2016.
Administración de MU	Los administradores que son miembros del grupo de funciones de "Administración de mensajería unificada" pueden administrar características de la organización de Exchange, como la configuración del servicio de mensajería unificada, las propiedades de mensajería unificada en los buzones, los mensajes de asistencia por voz de mensajería unificada y la configuración del operador automático para mensajería unificada.
Servicio de asistencia	De forma predeterminada, el grupo de funciones del servicio de asistencia permite a los miembros ver y modificar las opciones de Office Outlook en la Web de cualquier usuario de la organización. Estas opciones podrían incluir la modificación del nombre para mostrar, la dirección o el teléfono. No incluyen opciones que no están disponibles en las opciones de Outlook en la Web, como la modificación del tamaño de un buzón o la configuración de la base de datos de buzones en la que se encuentra un buzón.
Administración de higiene	Los administradores que pertenecen al grupo de roles "Administración de higiene" pueden configurar las funciones antivirus y contra correo electrónico no deseado de Exchange 2016. Los programas de terceros que se integran con Exchange 2016 pueden agregar cuentas de servicio a este grupo de roles para que dichos programas puedan tener acceso a los cmdlets que se requieren para recuperar y establecer la configuración de Exchange.
Administración de registros	Los usuarios que son miembros del grupo de funciones "Administración de registros" pueden configurar las características de cumplimiento, como las etiquetas de directiva de retención, las clasificaciones de mensajes y las reglas de transporte.
Administración de la detección	Los administradores o usuarios que son miembros del grupo de funciones de "Administración de la detección" pueden realizar búsquedas de buzones en la organización de Exchange para obtener datos que cumplan determinados criterios y pueden configurar retenciones legales de buzones de correo.
Administración de carpetas públicas	Los administradores que son miembros del grupo de roles "Administración de carpetas públicas" pueden administrar carpetas públicas en los servidores que ejecuten Exchange 2016.

Grupo de funciones integradas	Descripción
Administración de servidor	Los administradores que son miembros del grupo de roles "Administración de servidor" pueden establecer la configuración específica de servidor del servicio de transporte, la mensajería unificada, el acceso de clientes y las características de buzón, como copias de las bases de datos, certificados, colas de transporte y conectores de envío, directorios virtuales y protocolos de acceso de cliente.
Configuración delegada	Los administradores que pertenecen al grupo de funciones "Configuración delegada" pueden implementar servidores que ejecutan Exchange 2016 que ya han sido aprovisionados por un miembro del grupo de funciones "Administración de la organización".
Administración de cumplimiento	Los usuarios que pertenecen al grupo de roles de "Administración de cumplimiento" pueden configurar y administrar la configuración de cumplimiento de Exchange de acuerdo con la directiva de la organización.

6.7.2 DIRECTIVAS DE ASIGNACIÓN DE ROLES DE ADMINISTRACIÓN

Una directiva de asignación de funciones de administración es una colección de una o más funciones de administración de usuarios finales que permite a los usuarios finales administrar su propio buzón Microsoft Exchange Server 2016 y la configuración de un grupo de distribución.

Forman parte del modelo de permisos de control de acceso basado en funciones (RBAC) en Exchange 2016 y permiten controlar qué configuración de un buzón específico y un grupo de distribución podrán modificar los usuarios finales. Los diferentes grupos de usuarios pueden tener directivas de asignación de funciones especializadas.

Básicamente, las directivas asocian los roles de administración de usuarios finales a los usuarios, impidiendo la administración de características que no estén directamente asociadas con el usuario.

Cuando se crea una directiva de asignación de roles, se define todo lo que un usuario puede hacer con el buzón. Por ejemplo, una directiva de asignación de funciones puede permitir que un usuario establezca el nombre para mostrar, configure el correo de voz y las reglas de la bandeja de entrada. Otra directiva de asignación de funciones puede permitir que un usuario cambie la dirección, utilice la mensajería de texto y configure los grupos de distribución.

De forma predeterminada, cada usuario que tenga un buzón de correo de Exchange Server 2016, incluidos los administradores, tiene una directiva de asignación de roles.

Se puede establecer que una directiva se aplique de forma predeterminada, elegir el contenido de la directiva de asignación de roles, anular la directiva predeterminada en algunos buzones de correo o no asignar ninguna directiva de asignación de roles predeterminada.

La directiva predeterminada se asocia automáticamente con los nuevos buzones, a los que no se les ha asignado de forma explícita una directiva de asignación de roles en el momento de su creación.

Es por ello que, la directiva de asignación de roles predeterminada debe contener todos los permisos que deben aplicarse a la mayoría de los buzones.

El modo más habitual de administrar los permisos para que los usuarios administren las opciones de su propio buzón y grupos de distribución es asignando un usuario a una directiva.

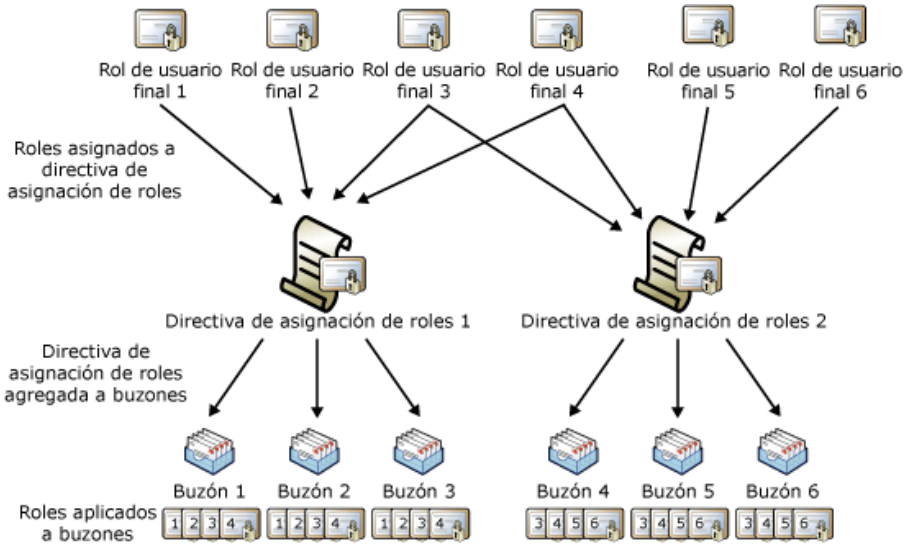
Cuando se asigna un rol de usuario final a una directiva de asignación de roles, todos los buzones asociados con la directiva reciben los permisos concedidos por el rol. Esto permite agregar o quitar permisos a conjuntos de usuarios sin tener que configurar buzones por separado.

En la siguiente imagen se puede observar que:

a) Los roles de usuario final se asignan a las directivas de asignación de roles. Las directivas de asignación de roles pueden compartir los mismos roles de usuario final.

b) Las directivas de asignación de roles se asocian con buzones. Cada buzón puede asociarse con una única directiva de asignación de roles.

c) Después de asociar un buzón con una directiva de asignación de roles, los roles de usuario final se aplican al buzón en cuestión. Los permisos concedidos por los roles se conceden al usuario del buzón.



Las directivas de asignación de roles constan de los siguientes componentes, que definen lo que los usuarios pueden hacer con sus buzones. Algunos de estos componentes se pueden aplicar también a grupos de funciones.

Cuando se usan con las directivas de asignaciones de roles, tales componentes están limitados para que los usuarios administren únicamente su propio buzón:

a) Buzón. A los buzones se les asigna una única directiva de asignación de funciones. Cuando se asigna una directiva de asignación de funciones a un buzón, se aplican al buzón las asignaciones entre funciones de administración y una directiva de asignación de funciones. Esto otorga al buzón todos los permisos proporcionados por las funciones de administración.

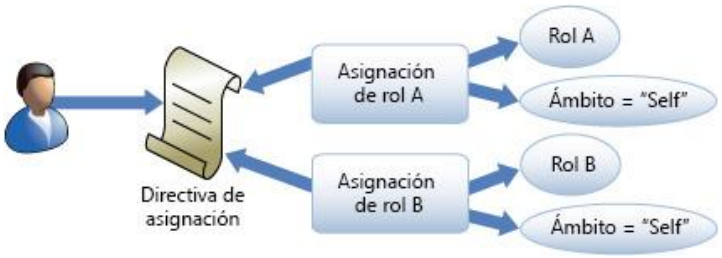
b) Directiva de asignación de roles de administración. La directiva de asignación de roles de administración es un objeto especial de Exchange 2016. Los usuarios se asocian con una directiva de asignación de funciones al crear sus buzones o si se cambia la directiva de asignación de funciones en un buzón. También es a lo que usted asigna funciones de administración de los usuarios finales. La combinación de todas las funciones en una directiva de asignación de funciones define todo lo que puede administrar un usuario en su buzón o grupo de distribución.

c) Función de administración. Una función de administración es un contenedor para una agrupación de entradas de funciones de administración. Las funciones se usan para definir tareas específicas que un usuario puede realizar en su buzón o en sus grupos de distribución. Una entrada de función de administración es un cmdlet, un script o un permiso especial que permite que se realice cada tarea específica en una función de administración. Solo se pueden usar funciones de administración de usuario final con directivas de asignación de funciones.

d) Asignación de roles de administración. Una asignación de funciones de administración es el vínculo entre una función de administración y una directiva de asignación de funciones. La asignación de una función de administración a una directiva de asignación de funciones garantiza la posibilidad de usar cmdlets y parámetros definidos en la función de administración. Cuando crea una asignación de funciones entre una directiva de asignación de funciones y una función de administración, no se puede especificar ningún ámbito. El ámbito predeterminado que aplica la asignación se basa en la función de administración y éste puede sólo ser "Self" o "MyGAL".

e) Entrada de función de administración. Las entradas de función de administración son entradas individuales de una función de administración que determinan qué cmdlets y qué parámetros están disponibles para la función de administración y el grupo de funciones. Cada entrada de función consiste en un único cmdlet y los parámetros a los que se puede tener acceso mediante la función de administración.

La siguiente imagen muestra cada capa de directiva de asignación de funciones de la lista anterior y cómo cada una de las capas se relaciona con la otra.



Por otro lado, la asignación directa de roles es un método avanzado mediante el cual se asignan roles de administración directamente a un usuario o grupo de seguridad universal sin usar un grupo de roles ni una directiva de asignación de roles. Las asignaciones directas de roles pueden resultar útiles cuando se debe proporcionar un conjunto de permisos pormenorizado a un usuario en concreto y no a otros.

Sin embargo, el uso de las asignaciones de funciones directas puede aumentar significativamente la complejidad del modelo de permisos y su mantenimiento a largo plazo. Si un usuario cambia de puesto de trabajo o deja la organización, se tendrá que eliminar manualmente las asignaciones y agregarlas al nuevo empleado. Por lo tanto, se recomienda usar los grupos de roles para asignar permisos a los administradores y usuarios especialistas, y las directivas de asignación de roles para asignar permisos a los usuarios.

6.7.3 ASIGNACIONES DE FUNCIONES DE DELEGACIÓN

Las asignaciones de funciones de delegación no proporcionan acceso para administrar las características, sino que, en su lugar, permiten que un usuario al que se asigna una función asigne la función especificada a otros usuarios.

Si el usuario al que se asigna una función es un grupo de funciones, cualquier miembro del grupo puede asignar la función a otro usuario al que se asigna una función.

De manera predeterminada, solamente el grupo de funciones de administración de la organización puede asignar funciones a otros usuarios a los que se asigna una función.

Así mismo, de forma predeterminada, solamente el usuario que instaló Exchange Server 2016 es miembro del grupo de funciones de administración de la organización. Sin embargo, si es necesario, se puede agregar otros usuarios a este grupo de funciones o crear otros grupos de funciones y asignar asignaciones de funciones de delegación a esos grupos.

Si se requiere que un usuario pueda administrar una característica determinada y asignar a otros usuarios una función que otorgue permisos para usar dicha característica, sería necesario realizar lo siguiente:

a) Una asignación de funciones normal para cada función de administración que otorga acceso a las características que deben administrarse.

b) Una asignación de funciones de delegación para cada función de administración que se permite asignar a otros usuarios a los que se asigna una función.

No es necesario que las asignaciones de funciones normales y de delegación para un usuario al que se asigna una función sean idénticas.

Por ejemplo, un usuario es un miembro de un grupo de funciones asignado a la función reglas de transporte mediante una asignación de funciones normal. Esto permite al usuario administrar la característica de reglas de transporte. Sin embargo, el usuario no tiene asignada una asignación de funciones de delegación para la función regla de transporte, por lo que no puede asignar esta función a otros usuarios.

6.7.4 AMBITOS EXCLUSIVOS

Los ámbitos exclusivos consisten en una clase especial de ámbito de administración explícito que se puede asociar con asignaciones de funciones de administración y que han sido diseñados para situaciones en las que existe un grupo con objetos de gran valor, por ejemplo, el buzón de correo de un presidente ejecutivo, el cual se requiere controlar estrechamente la obtención de acceso a dicho buzón para administrar esos objetos.

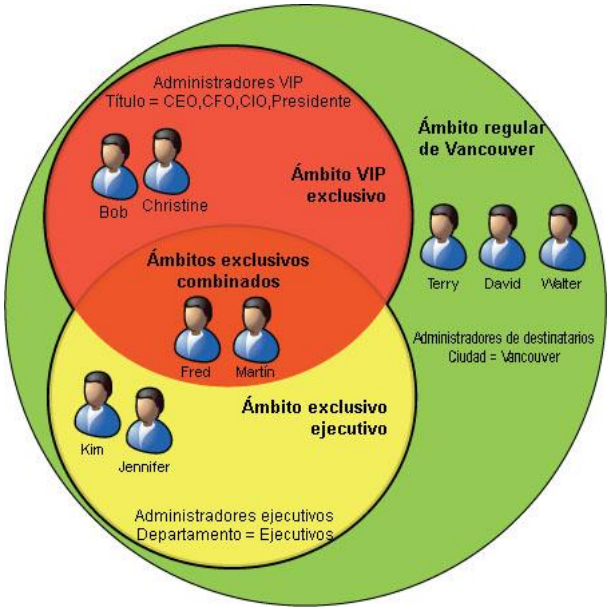
Al crear un ámbito exclusivo, los únicos que pueden modificar los objetos que concuerdan con el ámbito son quienes tienen asignados dicho ámbito exclusivo o uno equivalente.

Las asignaciones de funciones que no están asignadas a ese ámbito exclusivo o uno equivalente no pueden modificar los objetos que coincidan con el ámbito, ni siquiera, aunque sus propias funciones posean ámbitos que pudieran incluir los objetos.

Los ámbitos exclusivos, por lo tanto, anulan cualquier otro ámbito normal que no sea exclusivo. Es un comportamiento similar al modo de denegar una entrada de control de acceso (ACE) en funciones de lista de control de acceso de Directorio Activo.

Así mismo, los ámbitos exclusivos solo son válidos con funciones administrativas o de especialistas, no son aptos para funciones de usuario final.

La siguiente imagen muestra la interacción entre los ámbitos exclusivos y la relación con los ámbitos normales.



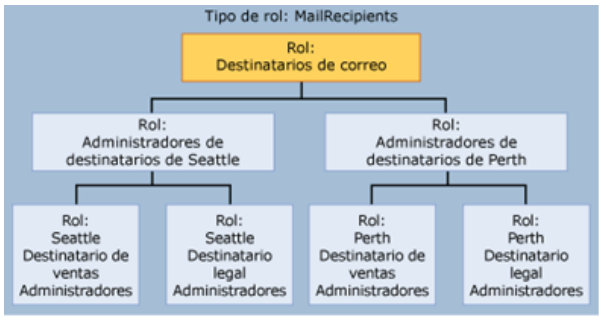
6.7.5 TIPOS DE FUNCIONES DE ADMINISTRACIÓN

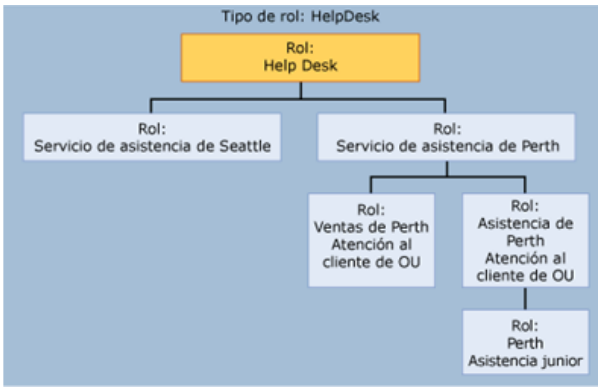
Los tipos de funciones de administración son la base de todas las funciones de administración. Definen los ámbitos implícitos definidos en todas las funciones de administración de un tipo de función específico y también actúan como agrupamiento lógico de las funciones relacionadas.

Todas las funciones de administración derivadas de la función de administración integrada principal tienen el mismo tipo de función.

En la siguiente imagen se muestra la relación jerárquica de varias funciones de administración. Las funciones "Destinatarios de correo" y "Servicio de asistencia" son funciones integradas.

Todas las funciones secundarias derivadas de estas funciones heredan el tipo de función de cada función integrada.





Los tipos de roles de administración también representan el conjunto máximo de cmdlets y sus parámetros que pueden agregarse a un rol asociado a un tipo de rol.

Los tipos de funciones de administración se dividen en las siguientes categorías:

a) Administrativa o experta. Las funciones relacionadas con un tipo de función administrativa o experta tienen un alcance más amplio en la organización de Exchange. Las funciones de este tipo habilitan tareas, como la administración de servidores o destinatarios, la configuración de organizaciones, la administración de cumplimiento y las auditorías, entre otras cosas.

b) Centrado en el usuario. Los roles asociados a un tipo de rol centrado en el usuario tienen un alcance estrechamente vinculado con un usuario individual. Las funciones de este tipo habilitan tareas, como la configuración y la autoadministración del perfil de usuario y la administración de grupos de distribución que pertenecen a usuarios, entre otras cosas. Los nombres de los roles asociados con los tipos de roles centrados en el usuario y los nombres de los tipos de roles centrados en el usuario comienzan con "My".

c) Específicos. Los roles asociados con tipos de roles específicos habilitan tareas que no son de tipo administrativo ni centrados en el usuario. Las funciones de este tipo habilitan tareas, como la suplantación de aplicaciones y el uso de cmdlets distintos de Exchange o scripts.

En la siguiente tabla, figuran todos los tipos administrativos de funciones de administración en Exchange 2016; asimismo, se indica si se aplica la configuración permitida por el tipo de función en toda la organización de Exchange o solamente en un servidor individual.

Tipo de función de administración	Roles integrados de administración	Descripción
ActiveDirectory Permissions	Función Permisos de Active Directory	Este tipo de función está asociado a funciones que les permiten a los administradores configurar permisos de Active Directory en una organización. Algunas de las características que utilizan permisos de Active Directory o una lista de control de acceso (ACL) incluyen conectores de envío y recepción de transporte, y permisos Enviar como y Enviar en nombre de para los buzones.
AddressLists	Función Listas de direcciones	Este tipo de rol se asocia con roles que les permiten a los administradores administrar listas de direcciones, listas globales de direcciones (LGD) y listas de direcciones sin conexión en una organización.
Application Impersonation	Función Application Impersonation	Este tipo de rol está asociado con roles que permiten a las aplicaciones usurpar la identidad de los usuarios de una organización para realizar tareas en su nombre.
AuditLogs	Función Registros de auditoría	Este tipo de rol está asociado con roles que les permiten a los administradores administrar la configuración de registro de auditoría de administrador en una organización.
CmdletExtension Agents	Función Agentes de extensión de cmdlet	Este tipo de función está asociado a funciones que les permiten a los administradores administrar agentes de extensión de cmdlets en una organización.

Tipo de función de administración	Roles integrados de administración	Descripción
Database AvailabilityGroups	Función Grupos de disponibilidad de base de datos	Este tipo de rol está asociado con funciones que les permiten a los administradores administrar grupos de disponibilidad de bases de datos (DAG) en una organización. Los administradores que tienen asignada esta función directa o indirectamente son los administradores de nivel más alto responsables de la configuración de alta disponibilidad en una organización.
DatabaseCopies	Función Copias de base de datos	Este tipo de función está asociado a funciones que les permiten a los administradores administrar copias de bases de datos en servidores individuales.
Databases	Función Bases de datos	Este tipo de función está asociado a funciones que les permiten a los administradores crear, administrar, instalar y desinstalar bases de datos de buzones y carpetas públicas en servidores individuales.
DisasterRecovery	Función Recuperación ante desastres	Este tipo de rol está asociado con roles que les permiten a los administradores restaurar buzones y grupos de disponibilidad de bases de datos (DAG) en una organización.
DistributionGroups	Función de grupos de distribución	Este tipo de función está asociado a funciones que les permiten a los administradores crear y administrar grupos de distribución y miembros de grupos de distribución en una organización.
EdgeSubscriptions	Función Suscripciones perimetrales	Este tipo de función está asociado a funciones que les permiten a los administradores administrar la sincronización perimetral y la configuración de suscripciones entre servidores de transporte perimetral y servidores de transporte de concentradores en una organización.
EmailAddress Policies	Función Directivas de dirección de correo electrónico	Este tipo de función está asociado a funciones que les permiten a los administradores administrar directivas de direcciones de correo electrónico en una organización.
Exchange Connectors	Función Conectores de Exchange	Este tipo de función está asociado a funciones que les permiten a los administradores administrar conectores distintos de los conectores de envío y recepción en una organización. Estos conectores incluyen conectores para grupo de enrutamiento y conectores de agente de entrega.
ExchangeServer Certificates	Función Certificados del servidor de Exchange	Este tipo de función está asociado a funciones que les permiten a los administradores crear, importar, exportar y administrar certificados de servidor de Exchange en servidores individuales.
ExchangeServers	Función Servidores de Exchange	Este tipo de función está asociado a funciones que les permiten a los administradores administrar la configuración del servidor Exchange en servidores individuales.

Tipo de función de administración	Roles integrados de administración	Descripción
ExchangeVirtual Directories	Función Directorios virtuales de Exchange	Este tipo de rol se asocia a roles que les permiten a los administradores administrar Microsoft Office Outlook en la Web, Microsoft ActiveSync, la Libreta de direcciones sin conexión (OAB), Detección automática, Windows PowerShell y directorios virtuales de la interfaz web de administración en servidores individuales.
FederatedSharing	Función Uso compartido federado	Este tipo de función está asociado a funciones que les permiten a los administradores administrar elementos compartidos entre bosques y entre organizaciones en una organización.
InformationRights Management	Función Administración de derechos de información	Este tipo de función está asociado a funciones que les permiten a los administradores administrar las características de Information Rights Management (IRM) de Exchange en una organización.
Journaling	Función Registro en diario	Este tipo de función está asociado a funciones que les permiten a los administradores administrar la configuración de registro en diario en una organización.
LegalHold	Función Retención legal	Este tipo de función está asociado a funciones que les permiten a los administradores realizar tareas de configuración si los datos de un buzón deben conservarse para litigios en una organización.
MailboxImport Export	Función Importar o exportar buzones	Este tipo de rol está asociado con los roles que permiten a los administradores importar y exportar contenido de buzones de correo y purgar el contenido no deseado de un buzón.
MailboxSearch Application	Función Búsqueda entre buzones para aplicaciones	Este tipo de rol está asociado a roles que permiten que las aplicaciones asociadas establezcan y vean el estado de retención legal de un buzón de correo de una organización.
MailboxSearch	Función Búsqueda entre buzones	Este tipo de función está asociado a funciones que les permiten a los administradores buscar el contenido de uno o más buzones en una organización.
MailEnabled PublicFolders	Función Carpetas públicas habilitadas para correo	Este tipo de función está asociado a funciones que les permiten a los administradores realizar tareas de configuración si las carpetas públicas individuales están habilitadas o deshabilitadas para correo en una organización. Este tipo de función le permite administrar las propiedades de correo electrónico solamente en las carpetas públicas. No le permite administrar las propiedades de las carpetas públicas que no son propiedades del correo electrónico. Para administrar propiedades de carpetas públicas ajenas que no son propiedades de correo electrónico, se le debe asignar un rol asociado a un tipo de rol de PublicFolders.

Tipo de función de administración	Roles integrados de administración	Descripción
MailRecipient Creation	Función Creación de destinatarios de correo	Este tipo de función está asociado a funciones que les permiten a los administradores crear y administrar buzones, contactos de correo, grupos de distribución y grupos de distribución dinámicos en una organización. Las funciones asociadas a este tipo de función se pueden combinar con funciones asociadas al tipo de función de MailRecipients para habilitar la creación y la administración de destinatarios. Este tipo de función no le permite habilitar carpetas públicas para el correo. Para habilitar carpetas públicas para el correo, se le debe asignar una función asociada al tipo de función de MailEnabledPublicFolders. Si su organización mantiene un modelo de permisos divididos en el que la creación de destinatarios la realiza un grupo distinto del que realiza la administración de destinatarios, asigne el rol MailRecipientCreation al grupo que realiza la creación de destinatarios y el rol MailRecipients al grupo que realiza la administración de destinatarios.
MailRecipients	Función Destinatarios de correo	Este tipo de función está asociado a funciones que les permiten a los administradores administrar buzones, usuarios de correo, contactos de correo, grupos de distribución y grupos de distribución dinámicos existentes en una organización. Las funciones asociadas a este tipo de función no pueden crear estos destinatarios, pero pueden combinarse con funciones asociadas al tipo de función de MailRecipientCreation para habilitar la creación y la administración de destinatarios. Este tipo de función no lo habilita a administrar carpetas públicas habilitadas para correo o grupos de distribución. Para administrar carpetas públicas habilitadas para correo, se le debe asignar una función asociada al tipo de función de MailEnabledPublicFolders. Para administrar grupos de distribución, debe recibir una función asociada al tipo de función de DistributionGroups. Si su organización mantiene un modelo de permisos divididos en el que la creación de destinatarios la realiza un grupo distinto del que realiza la administración de destinatarios, asigne el rol MailRecipientCreation al grupo que realiza la creación de destinatarios y el rol MailRecipients al grupo que realiza la administración de destinatarios.
MailTips	Función Sugerencias para correo electrónico	Este tipo de rol está asociado con roles que les permiten a los administradores administrar las sugerencias de correo en una organización.

Tipo de función de administración	Roles integrados de administración	Descripción
MessageTracking	Función Seguimiento de mensajes	Este tipo de función está asociado a funciones que les permiten a los administradores realizar un seguimiento de los mensajes en una organización.
Migration	Función Migración	Este tipo de función está asociado a funciones que les permiten a los administradores migrar buzones y el contenido de los buzones hacia un servidor o fuera de él.
Monitoring	Función Supervisión	Este tipo de función está asociado a funciones que les permiten a los administradores supervisar los servicios de Microsoft Exchange y la disponibilidad de componentes en una organización. Además de los administradores, las funciones asociadas a este tipo de función pueden usarse con la cuenta de servicio usada por las aplicaciones de supervisión a fin de recopilar información acerca del estado de los servidores Exchange.
MoveMailboxes	Función Mover buzones	Este tipo de función está asociado a funciones que les permiten a los administradores mover buzones entre servidores en una organización y entre servidores en la organización local y otra organización.
OfficeExtension Application	Rol OfficeExtension Application	Este tipo de rol está asociado a roles que permiten que las aplicaciones de extensiones de Microsoft Office accedan a los buzones de correo de los usuarios de una organización.
OrgCustomApps	Rol Aplicaciones personalizadas de la organización	Este tipo de rol está asociado a roles que permiten a los administradores ver y modificar las aplicaciones personalizadas de su organización.
OrgMarketplace Apps	Rol de aplicaciones de la tienda de la organización	Este tipo de rol está asociado a roles que permiten a los administradores ver y modificar las aplicaciones del catálogo de soluciones de su organización.
Organization ClientAccess	Función Acceso de clientes de la organización	Este tipo de función está asociado a funciones que les permiten a los administradores administrar la configuración del servidor de acceso de cliente en una organización.

Tipo de función de administración	Roles integrados de administración	Descripción
Organization Configuration	Función Configuración de la organización	Este tipo de función está asociado a funciones que les permiten a los administradores administrar las configuraciones de toda una organización. La configuración de la organización que se puede controlar con este tipo de función incluye lo siguiente (entre otras cosas): Si se habilitan o deshabilitan las sugerencias de correo electrónico para la organización. La dirección URL de la página principal de la carpeta administrada. La dirección de destinatario SMTP de Microsoft Exchange y las direcciones de correo electrónico alternativas. La configuración de esquema de propiedades del buzón de recursos. Las direcciones URL de ayuda de la Consola de administración de Exchange y Outlook en la Web. Este tipo de función no incluye los permisos incluidos en los tipos de función OrganizationClientAccess o OrganizationTransportSettings.
Organization TransportSettings	Función Configuración de transporte de la organización	Este tipo de función está asociado a funciones que les permiten a los administradores administrar las configuraciones de transporte de toda la organización, como los mensajes del sistema, la configuración del sitio y otras configuraciones de transporte de toda la organización. Esta función no permite crear ni administrar conectores de envío o recepción, colas, higiene, agentes, dominios remotos o aceptados, ni reglas de transporte.
POP3AndIMAP4 Protocols	Función Protocolos POP3 e IMAP4	Este tipo de función está asociado a funciones que les permiten a los administradores administrar la configuración de POP3 e IMAP4, como los parámetros de autenticación y conexión de servidores individuales.
PublicFolders	Función Carpetas públicas	Este tipo de función está asociado a funciones que les permiten a los administradores administrar las carpetas públicas en una organización. Este tipo de función no le permite realizar tareas de administración si las carpetas públicas están habilitadas para correo, ni tampoco le permite administrar la replicación de carpetas públicas. Para habilitar o deshabilitar una carpeta pública para el correo, se le debe asignar una función asociada al tipo de función de MailEnabledPublicFolders. Para configurar la replicación de carpetas públicas, se le debe asignar una función asociada al tipo de función de PublicFolderReplication.

Tipo de función de administración	Roles integrados de administración	Descripción
Receive Connectors	Función Conectores de recepción	Este tipo de rol está asociado con roles que les permiten a los administradores administrar la configuración del conector de recepción de transporte, como los límites de tamaño de un servidor individual.
RecipientPolicies	Función Directivas de destinatarios	Este tipo de función está asociado a funciones que les permiten a los administradores administrar directivas de destinatarios, como las directivas de aprovisionamiento, en una organización.
RemoteAnd Accepted Domains	Función Dominios remotos y aceptados	Este tipo de función está asociado a funciones que les permiten a los administradores administrar dominios remotos y aceptados en una organización.
ResetPassword	Rol Restablecer contraseña	Este tipo de función está asociado a funciones que les permiten a los usuarios restablecer sus propias contraseñas y a los administradores, restablecer las contraseñas de los usuarios en una organización.
Retention Management	Función Administración de la retención	Este tipo de función está asociado a funciones que les permiten a los administradores administrar las directivas de retención en una organización.
Role Management	Función Administración de funciones	Este tipo de función está asociado a funciones que les permiten a los administradores administrar grupos de funciones de administración, directivas de asignación de funciones, funciones de administración, entradas de funciones, asignaciones y ámbitos en una organización. Los usuarios a los que se asignaron funciones asociadas a este tipo de función pueden anular el grupo de funciones role group managed by, configurar cualquier grupo de funciones, y agregar miembros a cualquier grupo de funciones o quitarlos de él.
SecurityGroup CreationAnd Membership	Función Pertenencia y Creación de grupos de seguridad	Este tipo de función está asociado a funciones que les permiten a los administradores crear y administrar UGS y sus miembros en una organización. Si su organización mantiene un modelo de permisos divididos en los que la creación y la administración de USG son realizadas por un grupo diferente del que administra los servidores de Exchange, asigne roles asociados a este tipo de rol a ese grupo.
SendConnectors	Función Conectores de envío	Este tipo de función está asociado a funciones que les permiten a los administradores administrar los conectores de envío de transporte en una organización.
Support Diagnostics	Función Diagnósticos de soporte	Este tipo de función está asociado a funciones que les permiten a los administradores realizar diagnósticos avanzados con la dirección de los Servicios de soporte técnico de Microsoft en una organización.

Tipo de función de administración	Roles integrados de administración	Descripción
TeamMailboxes	Rol Buzones de equipo	Este tipo de rol se asocia a roles que permiten que las aplicaciones asociadas actualicen los estados de ciclo de vida de buzones de correo del sitio de una organización.
TeamMailbox Lifecycle Application	Rol TeamMailbox Lifecycle Application	Este tipo de rol se asocia a roles que permiten que las aplicaciones asociadas actualicen los estados de ciclo de vida de buzones de correo del sitio de una organización.
TransportAgents	Función Agentes de transporte	Este tipo de función está asociado a funciones que les permiten a los administradores administrar agentes de transporte en una organización.
TransportHygiene	Función Higiene de transporte	Este tipo de función está asociado a funciones que les permiten a los administradores administrar características de protección contra el correo no deseado y antivirus en una organización.
TransportQueues	Función Colas de transporte	Este tipo de función está asociado a funciones que les permiten a los administradores administrar colas de transporte en servidores individuales.
TransportRules	Función Reglas de transporte	Este tipo de función está asociado a funciones que les permiten a los administradores administrar reglas de transporte en una organización.
UMMailboxes	Función Buzones de MU	Este tipo de función está asociado a funciones que les permiten a los administradores administrar la configuración de mensajería unificada (MU) de los buzones y otros destinatarios en una organización.
UMPrompts	Función Mensajes de mensajería unificada	Este tipo de función está asociado a funciones que les permiten a los administradores crear y administrar mensajes de asistencia por voz de MU en una organización.
UnifiedMessaging	Función Mensajería unificada	Este tipo de función está asociado a funciones que les permiten a los administradores administrar los servidores de MU en una organización. Esta función no lo habilita a administrar la configuración de buzones específicos de mensajería unificada o mensajes de mensajería unificada. Para administrar la configuración específica del buzón de MU, utilice las funciones asociadas con el tipo de función UMMailboxes. Para administrar mensajes de MU, utilice las funciones asociadas con el tipo de función UMPrompts.
UnScopedRole Management	Función Administración de funciones sin ámbito	Este tipo de rol está asociado a funciones que les permiten a los administradores crear y administrar roles de administración de nivel superior sin ámbito en una organización.
UserOptions	Función Opciones de usuario	Este tipo de rol está asociado a roles que les permiten a los administradores ver las opciones de Outlook en la Web de un usuario en una organización. Los roles asociados a este tipo de rol pueden usarse para ayudar a un usuario a diagnosticar problemas con su configuración.

Tipo de función de administración	Roles integrados de administración	Descripción
UserApplication	Rol UserApplication	Este tipo de rol se asocia a roles que permiten que las aplicaciones asociadas actúen en nombre de los usuarios finales de una organización.
ViewOnlyAudit Logs	Rol View-Only Audit Logs	Este tipo de rol está asociado con roles que les permiten a los administradores buscar el registro de auditoría de administrador en una organización.
ViewOnly Configuration	Función Configuración con permiso de vista	Este tipo de función está asociado a funciones que les permiten a los administradores ver todas las opciones de configuración distintas de las de los destinatarios de Exchange en una organización. Ejemplos visibles de configuración son la configuración de servidores, la configuración de transporte, la configuración de bases de datos y la configuración de toda la organización. Las funciones asociadas a este tipo de función se pueden combinar con funciones asociadas al tipo de función de ViewOnlyRecipients para crear una función que pueda ver cada objeto de una organización.
ViewOnly Recipients	Función Destinatarios con permiso de vista	Este tipo de función está asociado a funciones que les permiten a los administradores ver la configuración de los destinatarios, como buzones, usuarios de correo, contactos de correo, grupos de distribución y grupos de distribución dinámicos. Las funciones asociadas a este tipo de función se pueden combinar con funciones asociadas al tipo de función de ViewOnlyConfiguration para crear una función que pueda ver cada objeto de la organización.
Workload Management	Rol Workload Management	Este tipo de rol está asociado a roles que permiten a los administradores administrar las directivas de administración de carga de trabajo de una organización. Los administradores pueden configurar las definiciones de estado de los recursos, las clasificaciones de carga de trabajo y habilitar o deshabilitar la administración de cargas de trabajo.

La siguiente tabla enumera todos los tipos de roles de administración centrados en el usuario y los roles de administración incorporados asociados en Microsoft Exchange Server 2016.

Tipo de función de administración	Roles integrados centrados en el usuario	Descripción
MyBaseOptions	MyBaseOptions	Este tipo de función está asociado a funciones que les permiten a los usuarios individuales ver y modificar la configuración básica de sus propios buzones y parámetros asociados.
MyContact Information	MyAddressInformation MyContactInformation MyMobileInformation MyPersonalInformation	Este tipo de función está asociado a funciones que les permiten a los usuarios individuales modificar su información de contacto. Esta información incluye la dirección y los números de teléfono.

Tipo de función de administración	Roles integrados centrados en el usuario	Descripción
MyCustomApps	Rol Mis aplicaciones personalizadas	Este tipo de rol está asociado a roles que permiten a los usuarios individuales ver y modificar sus aplicaciones personalizadas.
MyDiagnostics	MyDiagnostics	Este tipo de rol está asociado a roles que permiten a los usuarios individuales realizar diagnósticos básicos en sus buzones de correo, como recuperar información de diagnóstico del calendario
MyDistributionGroup Membership	MyDistributionGroup Membership	Este tipo de función está asociado a las funciones que les permiten a los usuarios individuales ver y modificar su membresía de grupos de distribución de una organización, siempre que dichos grupos de distribución permitan la manipulación de las membresías de los grupos.
MyDistributionGroups	MyDistributionGroups	Este tipo de función está asociado a funciones que les permiten a los usuarios individuales crear, modificar y ver grupos de distribución, y modificar, ver, quitar y agregar miembros en sus propios grupos de distribución.
MyProfileInformation	MyDisplayName MyName MyProfileInformation	Este tipo de función está asociado a funciones que les permiten a los usuarios individuales modificar su nombre.
MyMarketplaceApps	Rol My Marketplace Apps	Este tipo de rol está asociado a roles que permiten a los usuarios individuales ver y modificar sus aplicaciones del catálogo de soluciones
MyRetentionPolicies	MyRetentionPolicies	Este tipo de función está asociada a funciones que les permiten a los usuarios individuales ver sus etiquetas de retención, y ver y modificar los parámetros y los valores predeterminados de su etiqueta de retención.
MyTeamMailboxes	Rol MyTeamMailboxes	Este tipo de rol está asociado a roles que permiten a los usuarios individuales crear buzones de correo del sitio y conectarlos a los sitios de Microsoft SharePoint.
MyTextMessaging	MyTextMessaging	Este tipo de función está asociado a funciones que les permiten a los usuarios individuales crear, ver y modificar los parámetros de los mensajes de texto.
MyVoiceMail	MyVoiceMail	Este tipo de función está asociado a funciones que les permiten a los usuarios individuales ver y modificar los parámetros del correo de voz.

7. AUDITORÍA Y CONFORMIDAD

Desde que Microsoft lanzó públicamente las primeras versiones comerciales de Exchange Server, el ámbito normativo y de legislación que se aplica a las organizaciones ha cambiado sustancialmente. Hoy en día, cualquier organización pública o privada, debe cumplir con una multitud de requerimientos legales para la preservación de la información, control en el acceso a información sensible, o en materia de prevención de pérdida de datos.

No solo en España o en Europa, sino también a nivel internacional, la regulación es cada vez más exigente. Es por ello que, Exchange Server ha evolucionado, a lo largo de los años, en cada versión, pasando desde un simple gestor de correo electrónico a una solución completa de colaboración con herramientas integradas para el control y la protección de los datos.

Desde Exchange Server 2007, Microsoft han mejorado mucho las características de seguridad, auditoría y conformidad, como las que se indican a continuación:

a) Nuevo modelo de acceso basado en roles (RBAC).

b) Integración de IRM en Outlook en la Web y las reglas de transporte

c) Archivo personal.

d) e-Discovery.

e) Moderación de mensajes.

f) Cifrado automático de correo electrónico y mensajes de voz.

g) Políticas de retención de mensajes.

h) Mejoras en la auditoría de tareas administrativas.

i) Directiva de mensajería y conformidad.

j) Prevención de pérdida de datos (DLP)

k) Importantes mejoras en las reglas de trasporte.

l) Protección frente a código dañino.

m) Conector Microsoft Rights Management basado en la nube Microsoft Azure.

n) Archivado, retención y exhibición de documentos electrónicos locales.

o) Mejora en los informes de Auditoría desde EAC.

Como se puede observar, Microsoft Exchange Server 2016 continúa con la senda de mejora de las capacidades y herramientas en el ámbito de la auditoría y la conformidad, que se suma al sistema tradicional de registros de actividad que se recogen el visor de sucesos y en los registros de actividad para los servicios de correo a través de sus protocolos: Outlook Web App y Active Sync (registro HTTP en IIS), intercambio de correo (SMTP), etc.

Microsoft Exchange Server 2016 ha sido diseñado pensando en la seguridad y la capacidad para ofrecer a los administradores herramientas integradas para cumplir con las exigentes normativas de hoy en día en materia de protección de datos personales y retención de la información.

Es por ello que, ofrece características y funcionalidades que ayudan a capturar, proteger, modificar, retener y descubrir mensajes de correo electrónico en el buzón de un usuario a medida que los mensajes circulan hacia la organización, a través de la misma o bien cuando son generados desde ella.

La siguiente lista contiene varios ejemplos de las áreas en las que las características de conformidad de Exchange Server 2016 puede ayudar a cumplir o responder a los requisitos de proposición de prueba:

a) Directivas de retención de datos. A muchas organizaciones se les pide que conserven los datos durante un periodo determinado y luego los eliminen para velar por la privacidad.

b) Disposiciones de privacidad y confidencialidad. Las organizaciones transmiten cada día información delicada y confidencial por correo electrónico, hacia y desde personas o la propia organización. Estas organizaciones deben velar por la privacidad de las personas y la confidencialidad de las comunicaciones.

c) Muros éticos. A las organizaciones que trabajan con valores y otra información, que como las de índole financiera, se les exige a menudo que prohíban la comunicación entre grupos determinados de la propia organización.

d) Peticiones de proposición de prueba. A veces las organizaciones se enfrentan a litigios. Como parte de este proceso, las partes litigantes pueden solicitarse información entre sí. Debido a que la comunicación comercial se efectúa mayoritariamente por correo electrónico, cumplir con los requerimientos judiciales supone buscar en el contenido de los correos electrónicos, incluidos los mensajes y los datos adjuntos.

Para el cumplimiento de la normativa de una organización, Microsoft Exchange Server 2016 proporciona diferentes mecanismos de control y características concretas como las siguientes:

a) Reglas de transporte.

b) Registro en diario.

c) Administración de registros de mensajes (MRM).

d) Exhibición de documentos electrónicos en contexto.

e) Conservación local y retención por juicio.

f) Registro de auditoría de buzones de correo.

g) Clasificación de mensajes.

h) Archivo local.

i) Prevención de pérdida de datos (DLP).

j) Information Rights Management (IRM).

k) S/MIME.

l) Registro de auditoría de administrador.

7.1 REGLAS DE FLUJO DE CORREO

Aunque las reglas de flujo de correo (también conocidas como reglas de transporte) no son una novedad en Exchange Server 2016, sí que han sido mejoradas y reforzadas, con un mayor número de condiciones y acciones aplicables.

Con las reglas de flujo de correo se pueden buscar condiciones específicas para los mensajes que pasen por su organización y realizar acciones con ellos. Así mismo, las reglas de flujo de correo permiten aplicar directivas de mensajes a los mensajes de correo electrónico, asegurar mensajes, proteger sistemas de mensajes y evitar la fuga de información.

Hoy en día, muchas organizaciones deben aplicar directivas de mensajería para limitar la comunicación entre destinatarios y remitentes, tanto dentro como fuera de la organización. Además de limitar las interacciones entre personas, departamentos de la misma organización y entidades fuera de la organización, algunas organizaciones están, asimismo, sujetas a los siguientes requisitos de directivas de mensajería:

a) Prevenir que contenido inapropiado entre y salga de la organización.

b) Filtrar la información confidencial de la organización.

c) Efectuar el seguimiento de los mensajes que envían o reciben ciertas personas, o archivarlos.

d) Redireccionar los mensajes entrantes y salientes para inspeccionarlos antes entregarlos.

e) Aplicar avisos de declinación de responsabilidades a los mensajes conforme pasan por la organización.

Las reglas de flujo de correo permiten aplicar directivas de mensajería a los mensajes de correo electrónico que fluyen por la canalización de transporte en servidores de buzones y servidores perimetrales. Permiten que los administradores de TI cumplan las directivas de mensajería, protejan los mensajes y los sistemas de mensajería, y eviten la difusión no autorizada de información.

Las reglas de flujo de correo constan de los siguientes componentes:

a) **Condiciones.** Se utilizan para identificar los mensajes a los que se debe aplicar una acción de regla de transporte. Las condiciones constan de uno o varios predicados que especifican qué partes de un mensaje se deben examinar. Algunos predicados examinan los campos o los encabezados de los mensajes como, por ejemplo, Para, De o CC. Otros examinan características de los mensajes como el asunto, el cuerpo, los datos adjuntos, y el tamaño y la clasificación del mensaje. La mayoría de los predicados exigen que se especifique un operador de comparación como igual a, no igual a o contiene, y un valor de coincidencia.

b) **Excepciones.** Las excepciones se basan en los mismos predicados que sirven para crear las condiciones de las reglas de transporte. Sin embargo, a diferencia de las condiciones, las excepciones identifican aquellos mensajes a los que no se debe aplicar las acciones de una regla de transporte. Las excepciones invalidan las condiciones e impiden que se apliquen ciertas acciones a un mensaje de correo electrónico, aunque éste cumpla todas las condiciones configuradas.

c) **Acciones.** Se aplican a los mensajes que cumplen las condiciones y no cumplen ninguna excepción definida en la regla de transporte. Las reglas de transporte permiten realizar múltiples acciones: rechazar, eliminar o redirigir mensajes; agregar más destinatarios; agregar prefijos al asunto del mensaje; o insertar avisos de declinación de responsabilidades y firmas personalizadas en el cuerpo del mensaje.

d) **Propiedades.** Las propiedades especifican cuándo y cómo debe aplicarse la regla de flujo de correo, así como si se va a aplicar o probar durante el periodo de tiempo que se esté aplicando.

Las reglas de flujo de correo tienen las siguientes propiedades:

a) El orden en el que se procesan las reglas. La regla cuya prioridad es 0 se procesa primero, seguida por la regla cuya prioridad es 1 y así en adelante. Se puede cambiar la prioridad de las reglas ajustando el orden de las reglas en el EAC o cambiando la prioridad de las reglas individuales. Por ejemplo, si dispone de una regla para rechazar mensajes que incluyan un número de tarjeta de crédito y otra que exija su probación, deseará que se aplique primero la regla de rechazo y que dejen de aplicarse las demás.

b) El modo de la regla. Controla si se aplica o se prueba la regla:

   i. Realizar todas las acciones (Exigir).

   ii. No llevar a cabo acciones que afectan a la entrega de correo y notificación al remitente (Probar con sugerencias de directiva). Se puede notificar a los remitentes que pueden estar infringiendo una de las reglas, incluso ante de que envíen un mensaje ofensivo. Para ello, se puede configurar las sugerencias de directiva y establecer el modo de la regla. Las sugerencias de directiva son similares a las sugerencias de correo electrónico y se pueden configurar para presentar una breve nota en el cliente de Microsoft Outlook o de Outlook en Web que proporcione información sobre posibles infracciones de la directiva a un usuario que esté creando un mensaje.

   iii. No llevar a cabo acciones que afecten a la entrega de correo (Probar sin sugerencias de directiva). Esta opción se usa normalmente para probar una regla recién creada.

c) Periodo de tiempo. Se puede especificar la fecha y hora a la que se inicia y se detiene la regla.

d) La regla está habilitada o no. Se puede querer deshabilitar una regla hasta que esté listo para probarla.

e) Categoría de los informes de regla. Se puede especificar si desea incluir la regla en los informes de reglas y cómo debe clasificarse en los informes.

f) Qué hacer si se produce un error de procesamiento de reglas. Se puede especificar si en caso de producirse un error en el procesamiento de la regla, ésta debe omitirse.

g) Cómo evaluar la dirección del remitente. Se puede especificar si las condiciones relacionadas con la dirección del remitente deben coincidir con el valor del encabezado del mensaje, del sobre del mensaje o de ambos.

Todos los mensajes de la organización se evalúan en función de las reglas de transporte de la organización. Las reglas se procesan siguiendo el orden enumerado en la página "Reglas" de EAC, o en función del valor del parámetro "Prioridad" del Shell de administración de Exchange.

Así mismo, cada regla también ofrece la opción de impedir que se sigan procesando más reglas una vez se cumple dicha regla.

Los agentes de transporte aplican las reglas de transporte en el servicio de transporte de los servidores de buzones y en el servicio de transporte en los servidores de transporte perimetral.

Si bien su funcionalidad es similar, los agentes difieren entre sí en cuanto a los predicados y acciones que ofrecen, el evento de transporte en el que se desencadena cada uno de ellos, y la prioridad de cada uno respecto a otros agentes de transporte habilitados en ese servidor.

Además, desde el punto de vista del procesamiento, existen varios tipos de mensajes que pasan a través de una organización y que, por sus características, en algunos casos no es posible aplicar las reglas de transporte. En la tabla siguiente se muestran los tipos de mensajes que se pueden procesar mediante reglas de transporte.

Tipo de mensaje	¿Se puede aplicar una regla?
Mensajes normales. Mensajes que contienen un único formato de texto enriquecido (RTF), HTML, un cuerpo de mensaje de texto sin formato, o un conjunto multiparte o alternativo de cuerpos de mensaje.	Si
Mensajes cifrados (S/MIME).	Las reglas solo pueden acceder a los encabezados de sobre contenidos en los mensajes cifrados S/MIME y procesar los mensajes según las condiciones que se inspeccionan en los encabezados. No se pueden procesar las reglas con condiciones que requieran la inspección del contenido del mensaje o acciones que pueden modificar el contenido.
Mensajes con firma clara. Mensajes que se han firmado, pero no cifrado.	Si
Mensajes de correo electrónico de mensajería unificada. Mensajes creados o procesados por el servicio de mensajería unificada, como correo de voz, fax, notificaciones de llamadas perdidas y mensajes creados o reenviados usando Microsoft Outlook Voice Access.	Si
Anónimo	Si
Mensajes enviados por remitentes anónimos.	Si
Informes de lectura. Informes que se generan en respuesta a solicitudes de confirmación de lectura realizadas por los remitentes. Los informes de lectura tienen una clase de mensaje de IPM.Note*.MdnRead o IPM.Note*.MdnNotRead.	Si
Mensajes cifrados con IRM o cifrado de Office 365.	Las reglas siempre tienen acceso a los encabezados del sobre incluidos en los mensajes cifrados y procesar los mensajes según las condiciones que se inspeccionan en los encabezados. Para que una regla inspeccione o modifique el contenido cifrado con IRM o cifrado de Office 365, la organización debe: – Usar Exchange Server o Exchange Online. – Tener establecido el descifrado de transporte en Obligatorio u Opcional. El descifrado de transporte está establecido en Opcional de forma predeterminada. – Tener la clave de cifrado. También se puede crear una regla de transporte que descifre automáticamente los mensajes cifrados con IRM.

Cuando se define una regla de flujo de correo mediante una condición que amplía la pertenencia a un grupo de distribución, el servicio de transporte del servidor del buzón de correo que aplica la regla guarda en caché la lista de destinatarios resultante. A eso se le llama caché de grupos expandida, la cual también utiliza el agente de registro en diario, con el fin de evaluar la pertenencia al grupo para las reglas del diario.

De forma predeterminada, la caché de grupos expandida almacena la pertenencia a grupos durante cuatro horas. También se almacenan los destinatarios que devuelve el filtro de destinatarios de un grupo de distribución dinámico.

La caché de grupos expandida hace que sean innecesarias las consultas repetidos al Directorio Activo y, por lo tanto, el tráfico de red resultante de resolver las pertenencias a grupos.

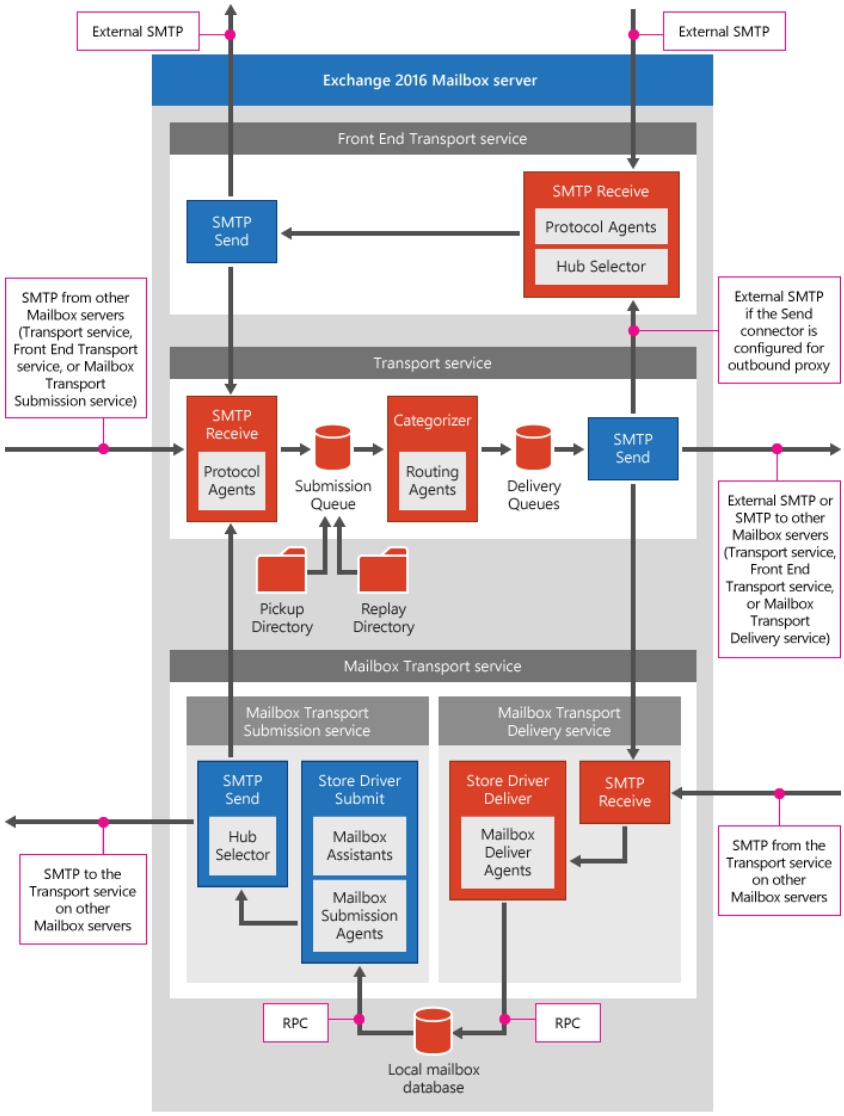
En Exchange Server 2016, este intervalo y otros parámetros relacionados con la caché de grupos expandida se pueden configurar. Es posible reducir el intervalo de expiración de caché o desactivar por completo el almacenamiento en caché, con el fin de garantizar que las pertenencias a grupos se actualizarán con mayor frecuencia.

Es necesario planear el correspondiente aumento de la carga de los controladores de dominio de Directorio Activo para las consultas de expansión de grupos de distribución. También es posible borrar la caché de un servidor buzón de correo reiniciando el servicio de transporte de Microsoft Exchange en ese servidor. Es necesario hacerlo en cada servidor buzón de correo en el que se desea borrar la caché.

Al crear y probar reglas de transporte que utilizan condiciones basadas en pertenencia a grupos de distribución, así como al solucionar problemas en esas reglas de transporte, también hay que tener en cuenta el impacto de la caché de grupos expandida.

Nota: Cuando se crea una regla de flujo de correo o se modifica o elimina una existente, el cambio se replica en todos los controladores de dominio de Directorio Activo de la organización. A continuación, todos los servidores de Exchange de la organización leen la nueva configuración en los servidores de Directorio Activo y aplican las reglas de flujo de correo nuevas o modificadas.

El agente de reglas de flujo de correo procesa las reglas de transporte en el servicio de transporte de los servidores de buzones. Se muestra resaltado en la siguiente imagen (en inglés).



Cuando se desencadena en el evento de transporte "OnRoutedMessage" se inicia el procesamiento de las reglas de transporte configuradas.

Es importante señalar que todos los mensajes de una organización de Exchange Server 2016 se ven afectados por al menos un servicio de transporte en un servidor de buzones, entre los que se encuentran:

a) Mensajes enviados y recibidos por usuarios del mismo sitio de Directorio Activo, incluidos los usuarios con buzones de correo en el mismo servidor de buzones de correo.

b) Mensajes enviados y recibidos por usuarios de distintos sitios de Directorio Activo.

c) Mensajes enviados y recibidos por usuarios de la organización de Exchange y usuarios externos.

Como ya se ha indicado anteriormente, las reglas de transporte configuradas en los servidores de buzones se almacenan en Directorio Activo. A ellas tienen acceso todos los servidores de buzones de la organización, puesto que la configuración se replica en todos los controladores de dominio de todo el bosque de Directorio Activo.

De esta forma, Exchange puede aplicar de forma coherente un único conjunto de reglas en toda la organización. Cada servidor de buzones realiza consultas en Directorio Activo para recuperar la configuración de reglas de transporte actual de la organización y aplicarlas a los mensajes que gestiona.

Por otro lado, el agente de reglas de transporte perimetrales procesa las reglas de transporte en los servidores perimetrales.

El servidor de transporte perimetral, que actúa como puerta de enlace de correo electrónico para sistemas de mensajería externos, es el lugar idóneo para aplicar procesos de higiene de mensajes y directivas de control al correo electrónico procedente de Internet.

Las reglas que aplica el agente de reglas de transporte perimetrales pueden reducir el número de total de mensajes que los servidores de buzones reciben y procesan y que, finalmente, se entregan a los destinatarios. También puede contribuir a eliminar contenido perjudicial o censurable de los mensajes. En la siguiente lista se ofrecen ejemplos de circunstancias en las que el agente de reglas perimetrales puede contribuir a proteger la organización:

a) **Ataques de virus.** Normalmente, suele transcurrir cierto tiempo entre el momento en que dicho tipo de código se detecta o se notifica, los proveedores de software antivirus lo identifican y crean las actualizaciones de software pertinentes, y los usuarios reciben el software antivirus actualizado. Esto provoca una laguna en la protección, por lo que un mensaje infectado puede entrar en la organización sin ser detectado.

b) **Ataques por denegación del servicio.** Los interesados en hacer daño a las organizaciones pueden utilizar este tipo de ataque, que puede llegar a hacer que servicios de red como el correo electrónico se deterioren, dejen de estar disponibles o experimenten interrupciones.

El agente de reglas perimetrales está diseñado para contribuir a reducir los efectos de cada uno de estos riesgos. También se puede someter el correo electrónico de Internet saliente al mismo tipo de escrutinio basado en directivas, de tal forma que el contenido malintencionado o censurable no salga de la organización. Además, el contenido de los mensajes se puede examinar para evitar que la información confidencial salga de la organización.

Las reglas de transporte configuradas en los servidores de transporte perimetral se almacenan en el servicio Active Directory Lightweight Directory Services (AD LDS), en cada servidor de transporte perimetral.

Nota: Las reglas configuradas en un servidor específico de transporte perimetral no se replican automáticamente en todos los servidores de este tipo que haya en la organización, ya sea con "EdgeSync" o sin él. Es posible que, en función de las necesidades, se requiera configurar todos los servidores de transporte perimetral con las mismas reglas de transporte o se tenga que configurar distintas reglas de transporte en cada uno de ellos para ajustarlas al patrón de tráfico de mensajes de correo electrónico propio de cada servidor.

Las condiciones y excepciones de las reglas de transporte constan de uno o más predicados, los cuales indican al agente de reglas de transporte de un servidor de buzones o el agente de reglas de transporte perimetral que examine una parte específica de un mensaje de correo electrónico, como el remitente, los destinatarios, el asunto, otros encabezados del mensaje y el cuerpo del mensaje, para determinar si la regla debe aplicarse a dicho mensaje.

Como tales, los predicados actúan como bloques de creación de condiciones y excepciones.

Para determinar si una regla de transporte debe aplicarse a un mensaje, la mayoría de los predicados disponen de una o más propiedades para las que es necesario especificar un valor.

El agente de reglas de transporte inspecciona las propiedades del mensaje para buscar los valores especificados. Por ejemplo, el predicado "HasClassification" requiere que se especifiquen una o más clasificaciones de mensajes para la propiedad de clasificación. Algunos predicados no tienen propiedades. Por ejemplo, el predicado "HasNoClassification" simplemente comprueba si el mensaje dispone de clasificación y, por lo tanto, no requiere de ningún valor.

7.1.1 CONDICIONES DE LAS REGLAS DE FLUJO DE CORREO

Para asignar un valor a un predicado, se debe determinar la propiedad o propiedades del predicado si dichos predicados requieren de más de una propiedad.

En las propiedades del Shell de administración de Exchange, las propiedades están disponibles como parámetros de los cmdlets "New-TransportRule" y "Set-TransportRule". Los valores de propiedad se especifican tras el nombre de propiedad.

A continuación, se muestra una tabla donde aparecen los predicados disponibles en un servidor de buzones:

a) La columna "Predicado" muestra el predicado tal como aparece en los asistentes para crear nuevas reglas de transporte y para editar reglas de transporte de la consola de administración de Exchange.

b) La columna "Nombre de predicado" muestra el nombre de predicado que devuelve el cmdlet "Get-TransportRulePredicate".

c) Las columnas "Propiedad de predicado" y "Segunda propiedad de predicado" muestran los tipos de propiedad. La mayoría de tipos de propiedad aceptan valores específicos.

Predicado en EAC	Nombre de predicado en Shell	Propiedad del predicado	Descripción
El remitente es.	From	Addresses	Esta condición encuentra los mensajes enviados por los buzones especificados, usuarios habilitados para correo o contactos.
El remitente está ubicado.	FromScope	FromUser Scope	Esta condición encuentra los mensajes enviados por remitentes incluidos en el ámbito especificado.
El remitente es un miembro de.	FromMemberOf	Addresses	Esta condición encuentra los mensajes en los que el remitente es miembro del grupo de distribución especificado.
La dirección del remitente incluye.	FromAddressContainsWords	Words	Esta condición encuentra los mensajes que contienen las palabras especificadas en la dirección del remitente.
La dirección del remitente coincide con.	FromAddress MatchesPatterns	Patterns	Esta condición encuentra los mensajes que contienen patrones de texto en la dirección del remitente que coinciden con la expresión regular especificada.

Predicado en EAC	Nombre de predicado en Shell	Propiedad del predicado	Descripción
Las propiedades especificadas del remitente incluyen cualquiera de estas palabras.	SenderADAttribute ContainsWords	Words	Esta condición encuentra los mensajes en los que el atributo especificado de un remitente contiene una cadena específica o una matriz de cadenas. Para aceptar varios valores, separe cada valor con una coma.
Las propiedades especificadas del remitente coinciden con estos patrones de texto.	SenderADAttribute MatchesPatterns	Patterns	Esta condición encuentra los mensajes en los que el atributo especificado del remitente contiene patrones de texto que coinciden con la expresión regular especificada.
El remitente ha invalidado las Sugerencias de directivas.	HasSenderOverride	No aplicable	Esta condición encuentra los mensajes donde el remitente ha elegido anular una directiva de DLP.
La dirección IP del remitente está en el rango.	SenderIPRanges	IPRanges	Esta condición encuentra los mensajes donde la dirección IP del remitente se encuentra dentro de los rangos especificados.
El dominio del remitente es.	SenderDomainIs	Nombre de dominio	Esta condición encuentra los mensajes donde el dominio o el subdominio del remitente coincide con el nombre de dominio especificado.
El destinatario es.	SentTo	Addresses	Esta condición encuentra los mensajes en los que uno de los destinatarios es el buzón de correo, el usuario habilitado para correo o el contacto especificado. Los destinatarios especificados pueden figurar en los campos Para, CC o CCO.
El destinatario está ubicado.	SentToScope	ToUserScope	Esta condición encuentra los mensajes enviados a destinatarios dentro del ámbito especificado.
El destinatario es un miembro de.	SentToMemberOf	Addresses	Esta condición encuentra los mensajes que contienen destinatarios que son miembros del grupo de distribución especificado. El grupo de distribución se pueden incluir en los campos Para, CC o CCO.
La dirección del destinatario incluye.	RecipientAddress ContainsWords	Words	Esta condición encuentra los mensajes en los que la dirección del destinatario contiene cualquiera de las palabras especificadas.

Predicado en EAC	Nombre de predicado en Shell	Propiedad del predicado	Descripción
La dirección del destinatario coincide con.	RecipientAddress MatchesPatterns	Patterns	Esta condición encuentra los mensajes en los que la dirección de un destinatario coincide con una expresión regular especificada.
Las propiedades especificadas del destinatario incluyen cualquiera de estas palabras.	RecipientAD AttributeContains Words	Words	Esta condición encuentra los mensajes en los que el atributo especificado de un destinatario contiene cualquiera de las palabras especificadas.
Las propiedades especificadas del destinatario coinciden con estos patrones de texto.	RecipientAD AttributeMatches Patterns	Patterns	Esta condición encuentra los mensajes en los que el atributo especificado de un destinatario coincide con una expresión regular especificada.
El dominio de un destinatario es.	RecipientDomainIs	Nombre de dominio	Esta condición encuentra los mensajes donde el dominio o subdominio de cualquier destinatario de mensaje coincide con el nombre de dominio especificado.
El asunto o el cuerpo incluye.	SubjectOrBody ContainsWords	Words	Esta condición encuentra los mensajes que tienen las palabras especificadas en el campo Asunto o en el cuerpo del mensaje.
El asunto o el cuerpo coincide con.	SubjectOrBody MatchesPatterns	Patterns	Esta condición encuentra los mensajes en los que los patrones de texto del campo Asunto o del cuerpo del mensaje coinciden con una expresión regular especificada.
El asunto incluye.	SubjectContains Words	Words	Esta condición encuentra los mensajes que tienen las palabras especificadas en el campo Asunto.
El asunto coincide con.	SubjectMatches Patterns	Patterns	Esta condición encuentra los mensajes en los que los patrones de texto del campo Asunto coinciden con una expresión regular especificada.
Activar esta regla en la siguiente fecha.	ActivationDate	No aplicable	Esta condición encuentra los mensajes que tendrán efecto después de una fecha específica.
Desactivar esta regla en la siguiente fecha.	ExpiryDate	No aplicable	Esta condición encuentra los mensajes que hacen que la regla detenga el procesamiento en una fecha específica.

Predicado en EAC	Nombre de predicado en Shell	Propiedad del predicado	Descripción
El contenido de algún documento adjunto incluye.	Attachment ContainsWords	Words	Esta condición encuentra los mensajes con datos adjuntos que contienen una cadena especificada.
Coincide con el contenido de cualquier documento adjunto.	Attachment MatchesPatterns	Patterns	Esta condición encuentra los mensajes con datos adjuntos que contienen patrones de texto que coinciden con una expresión regular especificada. Al intentar coincidir con un patrón, solo se examinan los primeros 150 KB de los datos adjuntos.
El contenido de cualquier documento adjunto no se puede inspeccionar.	AttachmentIs Unsupported	No aplicable	Esta condición encuentra los mensajes cuyos datos adjuntos no están admitidos.
El nombre del archivo adjunto coincide con.	AttachmentNameM atchesPatterns	Patterns	Esta condición encuentra los mensajes que contienen patrones de texto en un nombre de archivo de datos adjuntos que coinciden con una expresión regular especificada.
La extensión del archivo adjunto coincide con.	Attachment ExtensionMatchesW ords	Words	Esta condición encuentra los mensajes que contienen datos adjuntos cuya extensión coincide con cualquiera de las palabras especificadas.
El tamaño de cualquier documento adjunto es mayor o igual que.	AttachmentSize Over	Size	Esta condición encuentra los mensajes que contienen datos adjuntos iguales o mayores al valor especificado.
El mensaje no finalizó el análisis.	Attachment ProcessingLimit Exceeded	No aplicable	Esta condición encuentra los mensajes para los que el motor de reglas no pudo completar la detección de los datos adjuntos. Esta condición se puede usar para crear reglas que colaboren con otras reglas de procesamiento de datos adjuntos y permite administrar mensajes cuyo contenido no se puede examinar por completo.

Predicado en EAC	Nombre de predicado en Shell	Propiedad del predicado	Descripción
Cualquier documento adjunto tiene contenido ejecutable.	AttachmentHas ExecutableContent	No aplicable	Esta condición encuentra los mensajes que contienen archivos ejecutables como datos adjuntos. El sistema usa la detección automática de tipos de archivos al inspeccionar las propiedades de archivo y no la extensión de archivo, lo que impide que los spammers puedan eludir el filtrado de reglas de transporte cambiando el nombre de la extensión de archivo.
Todos los datos adjuntos están protegidos con contraseña.	AttachmentIs PasswordProtected	No aplicable	Esta condición encuentra los mensajes que contienen datos adjuntos con archivos comprimidos protegidos con contraseña y, por lo tanto, no se pueden examinar.
El mensaje contiene información confidencial.	MessageContains DataClassifications	Sensitive Information	Esta condición encuentra los mensajes que contienen información confidencial. Esta condición es necesaria en reglas que usan la acción NotifySender (Notificar al remitente con una sugerencia de directiva).
El cuadro Para contiene.	AnyOfToHeader	Addresses	Esta condición encuentra los mensajes en los que el campo Para incluye a alguno de los destinatarios especificados.
El cuadro Para contiene a un miembro de.	AnyOfToHeader MemberOf	Addresses	Esta condición encuentra los mensajes en los que el campo Para contiene un destinatario miembro del grupo de distribución especificado.
El cuadro CC contiene.	AnyOfCcHeader	Addresses	Esta condición encuentra los mensajes en los que el campo CC incluye a alguno de los destinatarios especificados.
El cuadro CC contiene a un miembro de.	AnyOfCcHeader MemberOf	Addresses	Esta condición encuentra los mensajes en los que el campo CC contiene un destinatario miembro del grupo de distribución especificado.
El cuadro Para o CC contiene.	AnyOfToCcHeader	Addresses	Esta condición encuentra los mensajes en los que los campos Para o CC incluye a alguno de los destinatarios especificados.
El cuadro Para o CC contiene un miembro de.	AnyOfToCcHeaderMemberOf	Addresses	Esta condición encuentra los mensajes en los que los campos Para o CC contienen un destinatario miembro del grupo de distribución especificado.

Predicado en EAC	Nombre de predicado en Shell	Propiedad del predicado	Descripción
El tamaño del mensaje es mayor o igual que.	MessageSizeOver	Size	Esta condición encuentra los mensajes cuyo tamaño general es igual o mayor que el valor especificado.
El nombre del conjunto de caracteres del mensaje incluye alguna de estas palabras.	ContentCharacterSetContainsWords	Juegos de caracteres	Esta condición encuentra los mensajes que contienen alguno de los nombres de conjuntos de caracteres especificados.
El remitente es uno de los destinatarios.	SenderManagementRelationship	ManagementRelationship	Esta condición encuentra los mensajes en los que el remitente tiene la relación de administración especificada con un destinatario.
El mensaje es entre miembros de estos grupos.	BetweenMember Of1 y BetweenMemberOf2	–Primera propiedad: Direcciones (BetweenMemberOf1) –Segunda propiedad: Direcciones (BetweenMemberOf2)	Esta condición encuentra los mensajes que se envían entre miembros de dos grupos de distribución.
El administrador del remitente o destinatario es.	ManagerForEvaluatedUser y ManagerAddress	–Primera propiedad: Evaluated User (ManagerForEvaluatedUser) –Segunda propiedad: Direcciones (Manager Addresses)	Esta condición encuentra los mensajes en los que el administrador del usuario especificado (remitente o destinatario) aparece en la lista de direcciones especificada.
Propiedad del remitente y cualquier destinatario compara como.	ADAttribute Comparison Attribute y ADComparison Operator	–Primera propiedad: ADAttribute (AD Comparison Attribute) –Segunda propiedad: Evaluation (AD Comparison Operator)	Esta condición encuentra los mensajes en los que el atributo Active Directory especificado del remitente coincide o no (según se especifique en la propiedad Evaluation) con el mismo atributo de alguno de los destinatarios.
El tipo de mensaje es	MessageType Matches	MessageType	Esta condición encuentra los mensajes del tipo especificado.

Predicado en EAC	Nombre de predicado en Shell	Propiedad del predicado	Descripción
El mensaje se clasifica como.	HasClassification	Classification	Esta condición encuentra los mensajes que tienen la clasificación especificada.
El mensaje no está marcado con ninguna clasificación.	HasNoClassification	No aplicable	Esta condición encuentra los mensajes que no tienen una clasificación de mensaje.
El mensaje tiene un SCL mayor o igual que.	SCLOver	SclValue	Esta condición encuentra los mensajes que tienen asignado un nivel de confianza contra correo no deseado (SCL) igual o superior al valor especificado.
La importancia del mensaje se establece en.	WithImportance	Importancia	Esta condición encuentra los mensajes marcados con la prioridad especificada.
Un encabezado de mensaje incluye.	HeaderContains MessageHeader y HeaderContains Words	–Primera propiedad: Message Header (Header Contains Message Header) –Segunda propiedad: Words (Header Contains Words)	Esta condición encuentra los mensajes donde el encabezado del mensaje especificado contiene una de las palabras especificadas.
Un encabezado de mensaje coincide.	HeaderMatches MessageHeader y HeaderMatches Patterns	–Primera propiedad: Message Header (Header Matches Message Header) –Segunda propiedad: Patterns (Header Matches Patterns)	Esta condición encuentra los mensajes donde el encabezado de mensaje especificado contiene un patrón de texto que coincide con una expresión regular especificada.

A continuación, se muestra una tabla donde aparecen los predicados disponibles en un servidor de en los servidores de transporte perimetral.

Predicado	Nombre de predicado en Shell	Propiedad del predicado	Descripción
Si el campo Asunto contiene palabras específicas.	SubjectContains	Words	SubjectContains coincide con los mensajes que contienen las palabras especificadas en el campo Asunto.
Si el campo Asunto o el cuerpo del mensaje contienen palabras específicas.	SubjectOrBody Contains	Words	SubjectOrBodyContains coincide con los mensajes que contienen las palabras especificadas en el campo Asunto o en el cuerpo del mensaje.
Si el encabezado de mensaje contiene palabras específicas.	HeaderContains	Message Header	HeaderContains coincide con los mensajes en los que el valor del encabezado de mensaje especificado contiene palabras específicas.
Si la dirección De contiene palabras específicas.	FromAddress Contains	Words	FromAddressContains coincide con los mensajes que contienen las palabras especificadas en el campo De.
Si la dirección de algún destinatario contiene palabras específicas.	AnyOfRecipient AddressContains Words	Words	AnyOfRecipientAddressContains coincide con los mensajes que contienen las palabras especificadas en los campos A, CC o CCO del mensaje.
Si el campo Asunto coincide con patrones de texto.	SubjectMatches	Patrones	SubjectMatches coincide con los mensajes en los que los patrones de texto del campo Asunto coinciden con una expresión regular especificada.
Si el campo Asunto o el cuerpo del mensaje coinciden con patrones de texto.	SubjectOrBody Matches	Patrones	SubjectOrBodyMatches coincide con los mensajes en los que los patrones de texto del campo Asunto o del cuerpo del mensaje coinciden con una expresión regular especificada.
Si el encabezado del mensaje coincide con patrones de texto.	HeaderMatches	Message Header	HeaderMatches coincide con los mensajes en los que el campo de encabezado de mensaje especificado contiene patrones de texto que coinciden con una expresión regular especificada.

Predicado	Nombre de predicado en Shell	Propiedad del predicado	Descripción
Si la dirección De coincide con patrones de texto.	FromAddress Matches	Patrones	FromAddressMatches coincide con los mensajes en los que los patrones de texto del campo De del mensaje coinciden con una expresión regular especificada.
Si alguna de las direcciones de destinatarios coincide con patrones de texto.	AnyOfRecipient AddressMatches	Patrones	AnyOfRecipientAddressMatches coincide con los mensajes cuyos patrones de texto de los campos Para, CC o CCO del mensaje coinciden con una expresión regular especificada.
Son un nivel de confianza contra correo no deseado (SCL) superior o igual al límite.	SCLOver	SclValue	SCLOver coincide con los mensajes con un SCL que es igual o mayor que el valor especificado.
Si el tamaño de alguno de los datos adjuntos es superior o igual al límite.	AttachmentSize Over	Size	AttachmentSizeOver coincide con los mensajes que contengan archivos adjuntos superiores al valor especificado.
Desde usuarios que están dentro o fuera de la organización.	FromScope	Ámbito	FromScope coincide con los mensajes que se envían desde el ámbito especificado.
El tamaño del mensaje es superior o igual al límite.	MessageSizeOver	Size	Esta condición encuentra mensajes cuyo tamaño es igual o mayor que el valor especificado.

Nota: Para más información consulte el siguiente enlace.
https://docs.microsoft.com/es-es/exchange/policy-and-compliance/mail-flow-rules/conditions-and-exceptions?view=exchserver-2016

7.1.2 ACCIONES DE LAS REGLAS DE FLUJO DE CORREO

Las acciones de regla de flujo de correo le permiten aplicar directivas de envío de mensajes a los mensajes de correo electrónico que fluyen por su organización y que coinciden con las condiciones y las excepciones definidas en las reglas de flujo de correo.

Cada acción de regla de flujo de correo contiene la acción y cualquier información necesaria para la acción.

A continuación, se muestra una lista con la información necesaria para cada una de las acciones disponibles en las reglas de flujo de correo.

Nombre de la acción	Nombre de la acción en Shell	Propiedades	Descripción
Reenviar el mensaje para su aprobación a estas personas	Moderate MessageByUser	Addresses	Reenvía el mensaje a los moderadores especificados en forma de datos adjuntos ajustados en una solicitud de aprobación. No se puede usar una lista de distribución como moderador.
Reenviar el mensaje para su aprobación al administrador del remitente	ModerateMessage ByManager	No aplicable	Reenvía el mensaje al administrador del remitente para su aprobación, si se rellenó el atributo de administrador en Directorio Activo.
Redirigir el mensaje a estos destinatarios	RedirectMessageTo	Addresses	Redirige el mensaje de correo electrónico a uno o más destinatarios especificados. El mensaje no se entrega a los destinatarios originales, y no se envía ninguna notificación al remitente ni a los destinatarios originales.
Rechazar el mensaje e incluir una explicación	RejectReason	RejectReason	Elimina el mensaje de correo electrónico y envía un informe de no entrega al remitente con el texto especificado como motivo del rechazo. El destinatario no recibe el mensaje ni la notificación.
Rechazar el mensaje con el código de estado mejorado de	RejectMessage EnhancedStatus Code	Enhanced StatusCode	Elimina el mensaje de correo electrónico y envía un informe de no entrega al remitente con el código de estado especificado. El destinatario no recibe el mensaje ni la notificación.
Eliminar el mensaje sin notificarlo a nadie	DeleteMessage	No aplicable	Elimina el mensaje de correo electrónico sin enviar ninguna notificación al destinatario ni al remitente.
Agregar destinatarios en el cuadro CCO	BlindCopyTo	Addresses	Agrega uno o más destinatarios como destinatarios con copia carbón oculta (CCO). Los destinatarios originales no reciben una notificación y no pueden ver las direcciones CCO.
Agregar destinatarios en el cuadro Para	AddToRecipient	Addresses	Agrega uno o más destinatarios al campo Para del mensaje. Los destinatarios originales pueden ver la dirección adicional.
Agregar destinatarios en el cuadro CC	CopyTo	Addresses	Agrega uno o más destinatarios al campo de copia carbón (CC) del mensaje. Los destinatarios originales pueden ver la dirección CC.

Nombre de la acción	Nombre de la acción en Shell	Propiedades	Descripción
Agregar el administrador del remitente como un destinatario	AddManagerAs RecipientType	Added RecipientType	Agrega el administrador del destinatario, si está definido en el atributo de administrador de Directorio Activo, como el tipo de destinatario especificado.
Aplicar un aviso de declinación de responsabilidades al mensaje (anexar un aviso)	ApplyHtml DisclaimerText ApplyHtm lDisclaimerText Location ApplyHtml DisclaimerFallback Action	–Primera propiedad: Disclaimer Text –Segunda propiedad: Fallback Action	Aplica un aviso de declinación de responsabilidades en HTML al mensaje. Hay tres parámetros en el Shell que corresponden a esta acción. Cuando se anexa un aviso de exención de responsabilidad, la propiedad ApplyHtmlDisclaimerTextLocation se establece en Append.
Aplicar un aviso de declinación de responsabilidades al mensaje (anteponer un aviso)	ApplyHtml DisclaimerText ApplyHtml DisclaimerText Location ApplyHtml DisclaimerFallback Action	–Primera propiedad: Disclaimer Text –Segunda propiedad: Fallback Action	Aplica un aviso de declinación de responsabilidades en HTML al mensaje. Hay tres parámetros en el Shell que corresponden a esta acción. Cuando se antepone un aviso de exención de responsabilidad, la propiedad ApplyHtmlDisclaimerTextLocation se establece en Prepend.
Quitar un encabezado de mensaje	RemoveHeader	Message Header	Quita el encabezado del mensaje especificado de un mensaje.
Establecer un encabezado de mensaje	SetHeaderName SetHeaderValue	–Primera propiedad: Message Header –Segunda propiedad: HeaderValue	Crea un nuevo encabezado de mensaje o modifica uno existente y configura el valor de ese encabezado de mensaje con el valor especificado. El Shell incluye dos parámetros con los que se puede realizar esta acción.
Aplicar una clasificación de mensajes	ApplyClassification	Classification	Aplica una clasificación de mensaje al mensaje.
Establecer el nivel de confianza contra correo no deseado (SCL)	SetScl	SclValue	Esta acción establece el nivel de confianza contra correo no deseado (SCL) en un mensaje de correo electrónico.
Anteponer al asunto del mensaje	PrependSubject	Prefix	Antepone al asunto del mensaje el texto especificado.
Aplicar protección de derechos	ApplyRightsProtecti onTemplate	RMSTemplatel dentity	Aplica al mensaje la plantilla de Rights Management Services (RMS) especificada.

Nombre de la acción	Nombre de la acción en Shell	Propiedades	Descripción
Requerir cifrado TLS	RouteMessage OutboundRequire Tls	Cualquiera de las siguientes: –Not applicable –Applicable	Fuerza el enrutamiento de los mensajes salientes a través de conexiones cifradas TLS.
Notificar al remitente con una sugerencia de directiva	NotifySender	NotifySender Type	Avisa al remitente cuando el mensaje infringe una directiva de DLP configurada en la organización. Cuando se utiliza esta acción, debe usar la condición MessageContainsDataClassification.
Generar informe de incidentes y enviarlo a	GenerateIncident Report	–Primera propiedad: Addresses –Segunda propiedad: Incident Report Content	Genera un informe del incidente y lo envía a los destinatarios especificados.
Detener el procesamiento de más reglas	StopRuleProcessing	No aplicable	Especifica si se debe detener el procesamiento de las reglas siguientes para este mensaje.

7.2 REGISTRO EN DIARIO

El registro en diario puede ayudar a la organización a responder a los requisitos de cumplimiento legal, normativo y organizativo mediante el registro de las comunicaciones de correo electrónico entrantes y salientes.

Al planear la retención y el cumplimento normativo de mensajes, es importante comprender el registro en diario, cómo se ajusta a las directivas de cumplimiento normativo de la organización y cómo Microsoft Exchange Server 2016 ayuda a asegurar los mensajes registrados en diario.

Existen dos sistemas para el almacenamiento de mensajes que proporciona Exchange Server 2016 y que tienden a confundirse: el registro en diario y el archivado.

a) **El registro en diario** es la capacidad de registrar todas las comunicaciones, incluyendo comunicaciones de correo electrónico, de una organización que se van a usar en la retención de correo electrónico de la organización o en la estrategia de archivado. Para cumplir con un mayor número de requisitos reglamentarios y de cumplimiento normativo, muchas organizaciones llevan registros de la comunicación que tiene lugar cuando los empleados llevan a cabo tareas cotidianas.

b) **Archivado** se refiere a la realización de copias de seguridad de los datos, eliminándolos de sus entornos nativos y almacenándolos en otro lugar, logrando así reducir la carga de su almacenamiento. Puede usar el registro en diario de Exchange como herramienta en la retención de correo electrónico o como estrategia de archivado.

Aunque ninguna normativa específica requiere el registro en diario, es posible que sea necesario realizarlo a fin del cumplimiento normativo de ciertas reglamentaciones.

En una organización de Exchange 2016, los servidores de buzones son los que gestionan todo el tráfico de correo electrónico. Todos los mensajes recorren al menos un servidor que ejecuta el servicio de transporte durante su vigencia y el agente de registro en diario es un agente de transporte centrado en el cumplimiento que procesa los mensajes de los servidores de buzones.

El agente se desencadena en los eventos de transporte "OnSubmittedMessage" y "OnRoutedMessage".

Así mismo, Exchange Server 2016 proporciona las siguientes opciones de registro en diario:

a) **Registro en diario estándar**. Esta opción se configura en una base de datos de buzones de correo. Permite al agente de registro en diario registrar todos los mensajes enviados o recibidos a través de los buzones ubicados en una base de datos de buzones de correo. Para registrar en diario todos los mensajes enviados y recibidos por todos los destinatarios y remitentes, se debe configurar el registro en diario para todas las bases de datos de buzones de todos los servidores de buzones de la organización.

b) **Registro en diario premium**. Esta opción permite, al agente de registro en diario, realizar registros más individualizados, mediante el uso de reglas de diario. En lugar de registrar en diario todos los buzones de una base de datos, es factible configurar reglas de diario que concuerden con las necesidades de la organización, registrando en diario destinatarios o miembros de grupos de distribución individuales. Para usar el registro en diario premium debe haber una licencia de acceso de cliente (CAL) de servidor empresarial de Exchange.

Cuando se habilita el registro en diario estándar en una base de datos de buzones de correo, esta información se guarda en Directorio Activo y el agente de registro en diario se encarga de su lectura. De manera similar, las reglas de diario configuradas con el registro en diario premium se guardan en Directorio Activo y el agente de registro en diario se encarga de aplicarlas.

Los aspectos clave de una regla de diario que es necesario comprender:

a) **Ámbito de regla de diario.** Define qué mensajes registrará el agente de registro en diario.

b) **Destinatarios del diario.** Especifica la dirección SMTP del destinatario que desee registrar en diario.

c) **Buzón de correo de registro en diario.** Especifica al menos uno de los buzones que se usan para recopilar informes de diario.

A través del ámbito se hace posible orientar una regla de diario a destinatarios internos, externos o globales. En la lista siguiente se describen estos ámbitos:

a) **Solo mensajes internos.** Se trata de las reglas de diario que tienen el ámbito establecido en mensajes internos del diario enviados entre los destinatarios de la organización de Exchange.

b) **Solo mensajes externos.** Se trata de las reglas de diario que tienen el ámbito establecido en mensajes externos del diario enviados a destinatarios o recibidos de remitentes ubicados fuera de la organización de Exchange.

c) **Todos los mensajes.** Se trata de las reglas de diario que tienen el ámbito establecido en todos los mensajes del diario que pasan por la organización independientemente de su origen o destino. Incluyen mensajes que ya han procesado las reglas de diario en los ámbitos interno y externo.

Se pueden implementar reglas de diario orientadas especificando la dirección SMTP del destinatario que se desea registrar en diario.

El destinatario puede ser un buzón de correo de Exchange, un grupo de distribución o un contacto. Estos destinatarios pueden estar sujetos a requisitos o pueden estar implicados en procedimientos legales en los que los mensajes de correo electrónico u otras comunicaciones se reúnan como evidencia.

Al asignar destinatarios específicos o grupos de destinatarios, se puede configurar fácilmente un entorno de registro de diario que coincida con los procesos de su organización y con los requisitos legales y normativos, al tiempo que se minimizan los costes de almacenamiento y otros costes relacionados con la retención de grandes cantidades de datos.

Se registrarán en diario todos los mensajes enviados o recibidos por los destinatarios que se hayan especificado en una regla de diario. Si se especifica un grupo de distribución como destinatario del diario, todos los mensajes que son enviados o recibidos por miembros del grupo de distribución, se registrarán en diario.

Si no se especifica ningún destinatario, se registrarán en diario todos los mensajes enviados o recibidos por los destinatarios que estén dentro del alcance de la regla de diario.

El buzón de correo de registro en diario se usa para recopilar informes de diario. La configuración de este buzón de correo de registro en diario depende de las directivas de la organización y de los requisitos legales y normativos. Puede especificarse un buzón de correo de registro en diario para reunir los mensajes de todas las reglas de diario configuradas en la organización, o pueden usarse buzones distintos para reglas de diario o grupos de reglas de diario distintos.

Los buzones de registro en diario contienen información muy confidencial por lo que se recomienda proteger activamente dichos buzones de registro en diario. Los mensajes contenidos en ellos pueden formar parte de procedimientos legales o estar sujetos a requisitos normativos. Es recomendable que se creen directivas que regulen quién puede obtener acceso a los buzones de registro en diario de su organización, limitando el acceso únicamente a aquellas personas que tengan necesidad directa de obtener acceso a ellos.

Un informe de diario es el mensaje que el agente de registro en diario genera en un servidor de buzones y que se envía al buzón de correo de registro en diario. El mensaje original se incluye sin modificaciones como dato adjunto al informe de diario. Este tipo de informe de diario se denomina un informe de diario de sobre.

Cuando se usa registro en diario estándar, se generan informes de diario para todos los mensajes que los buzones de correo enviaron o recibieron en una base de datos de buzones de correo habilitada para registro en diario. Cuando se usa registro en diario premium, se generan informes de diario para los mensajes que coinciden con una regla de diario.

La información que contiene un informe de diario se organiza para que todos los valores del campo de encabezado tengan su propia línea. Esto le permite analizar con facilidad los informes de diario en forma manual o mediante un proceso automatizado, en función de los requisitos.

Cuando el agente de registro en diario registra un mensaje, dicho agente intenta capturar la mayor cantidad de detalles posible del mensaje original. Esta información es muy importante a la hora de determinar la intención del mensaje, sus destinatarios y sus remitentes. Por ejemplo, si los destinatarios que se identifican en el mensaje están directamente especificados en el campo Para, el campo CC o están incluidos como parte de una lista de distribución, esto puede determinar la índole y el alcance de su participación en la comunicación por correo electrónico.

En función de la situación, Exchange Server 2016 podría generar más de un informe de diario para un único mensaje. El hecho de que un mensaje único genere uno o varios informes de diario depende de varios factores, como la bifurcación del mensaje o la expansión del grupo de distribución.

7.3 ADMINISTRACIÓN DE REGISTRO DE MENSAJES

La administración de registros de mensajes (MRM) es la tecnología de administración de registros en Microsoft Exchange Server 2016 que ayuda a las organizaciones a reducir los riesgos legales asociados con el correo electrónico.

La implementación de MRM puede ayudar a cumplir con diferentes escenarios y requisitos legales:

a) **Cumplir con los requisitos empresariales.** Según las directivas de mensajería de su organización, es posible que necesite conservar mensajes de correo electrónico importantes durante un período determinado.

b) **Cumplir con los requisitos legales y las normas de regulación.** Muchas organizaciones tienen un requisito legal o una norma de regulación para almacenar mensajes durante un período de tiempo concreto y eliminarlos pasado este. El almacenamiento de mensajes durante un período más largo del necesario puede incrementar los riesgos legales y financieros de su organización.

c) **Aumentar la productividad del usuario.** Si se deja sin administrar, el volumen del correo electrónico que incrementa constantemente los buzones de correo de los usuarios también puede tener un impacto en la productividad del usuario. El uso de MRM puede ayudar a disminuir el desorden de otros correos en la información de los buzones de los usuarios y, por lo tanto, aumentar la productividad.

d) **Mejorar la administración de almacenamiento.** Debido a las expectativas de los servicios de correo electrónico gratuitos para clientes, muchos usuarios conservan mensajes antiguos durante un largo período antes de eliminarlos. Mantener grandes buzones de correo se está convirtiendo en una práctica estándar, y no se debería forzar a los usuarios a cambiar sus hábitos de trabajo en base a las cuotas restrictivas del buzón de correo. Sin embargo, la retención de mensajes pasado el período necesario por razones empresariales, legales o normativas también incrementa los costes de almacenamiento.

Por todo ello, MRM facilita el mantenimiento de mensajes necesario para cumplir con directivas de la organización o las necesidades legales y ayuda a quitar el contenido que no disponga de valor legal o empresarial.

En Exchange Server 2016 esto se logra mediante el uso de etiquetas y directivas de retención. Las etiquetas y directivas de retención se usan para aplicar los ajustes de retención a un buzón de correo entero y a carpetas de buzones de correo predeterminados como los elementos eliminados y de la bandeja de entrada.

Cuando un mensaje alcanza su antigüedad de retención especificada en la etiqueta de retención aplicable, el Asistente para carpetas administradas realiza la acción de retención especificada en la etiqueta. Entonces, es posible eliminar los mensajes con la capacidad de recuperarlos o de forma permanente. Si se aprovisiona un archivo para el usuario, también es posible usar etiquetas de retención para mover elementos al archivo local.

La recomendación a la hora de diseñar una gestión MRM es la siguiente:

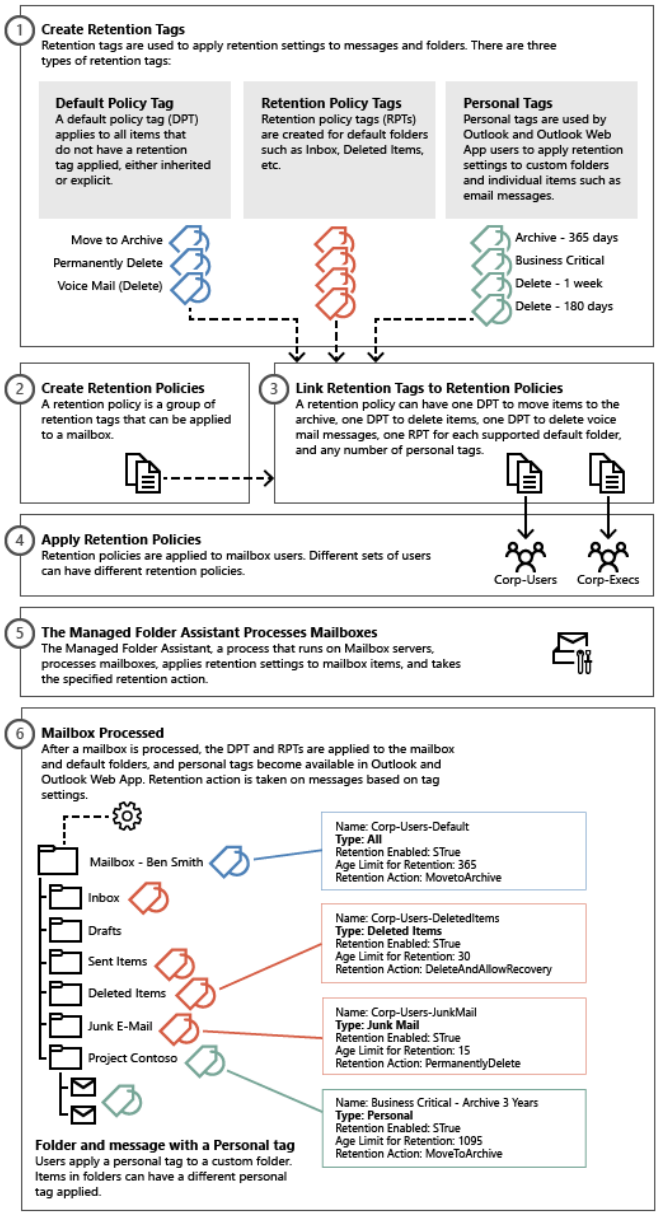
a) Asignar etiquetas de directiva de retención (RPT) a carpetas predeterminadas, como la bandeja de entrada y los elementos eliminados.

b) Aplicar etiquetas de directiva predeterminada (DPT) a los buzones de correo para administrar la retención de todos los elementos sin etiquetas.

c) Permitir al usuario asignar etiquetas personales a carpetas personalizadas y a elementos individuales.

d) Separar la funcionalidad MRM de la administración de la bandeja de entrada y de los hábitos de archivo de usuarios. No es necesario que los usuarios archiven mensajes en carpetas administradas en función de los requisitos de retención. Los mensajes individuales pueden tener una etiqueta de retención diferente de la etiqueta aplicada a la carpeta en la que se estos mensajes se encuentran.

La siguiente imagen muestra las tareas incluidas en la implementación de esta estrategia.



Como se puede observar, las etiquetas de retención se usan para aplicar la configuración de retención a carpetas y a elementos individuales como mensajes de correo electrónico y correo de voz.

Estas configuraciones especifican el tiempo que un mensaje permanece en un buzón de correo y la acción que se debe realizar cuando el mensaje alcanza la antigüedad de retención especificada. Cuando el mensaje alcanza la antigüedad de retención, se elimina o se mueve al buzón archivo local del usuario.

Las etiquetas de retención se clasifican en los siguientes tres tipos en función de quién puede aplicarlas y en qué parte de un buzón se puede aplicar.

Tipo de etiqueta de retención	Se aplica a	Aplicada por	Acciones disponibles	Detalles
Etiqueta de directiva predeterminada (DPT)	Automáticamente a todo el buzón. Las DPT se aplican a elementos sin etiquetar, que son elementos de buzón que no tienen aplicada una etiqueta de retención directamente o por herencia de la carpeta.	Administrador	– Mover a archivo. – Eliminar y permitir recuperación. – Eliminar permanente-mente.	Los usuarios no pueden cambiar las DPT aplicadas a un buzón.
Etiqueta de directiva de retención (RPT)	Automáticamente a una carpeta predeterminada (bandeja de entrada, elementos eliminados, elementos enviados, etc.)	Administrador	– Eliminar y permitir recuperación. – Eliminar permanente-mente.	Los usuarios no pueden cambiar la RTP aplicada a una carpeta predetermina da
Etiqueta personal	Manualmente a elementos y carpetas. Los usuarios pueden automatizar el etiquetado usando reglas de la bandeja de entrada para mover un mensaje a una carpeta que tenga una etiqueta determinada o para aplicar una etiqueta personal al mensaje.	Usuarios	– Mover a archivo. – Eliminar y permitir recuperación. – Eliminar permanente-mente.	Las etiquetas personales permiten a los usuarios determinar cuánto tiempo se debe retener un elemento.

La siguiente tabla enumera las etiquetas de retención predeterminadas vinculadas a la directiva MRM predeterminada.

Nombre	Tipo	Antigüedad de retención (días)	Acción de retención
Mover al archivo después de 2 años de forma predeterminada	DPT	730	Mover a archivo

Nombre	Tipo	Antigüedad de retención (días)	Acción de retención
Mover al archivo después de 1 año en forma personal	Etiqueta personal	365	Mover a archivo
Mover al archivo después de 5 años en forma personal	Etiqueta personal	1.825	Mover a archivo
Nunca mover al archivo en forma personal	Etiqueta personal	No aplicable	Mover a archivo
Mover elementos recuperables a archivo después de 14 días	Carpeta Elementos recuperables	14	Mover a archivo
Eliminar después de una semana	Etiqueta personal	7	Eliminar y permitir la recuperación
Eliminar después de un mes	Etiqueta personal	30	Eliminar y permitir recuperación
Eliminar después de seis meses	Etiqueta personal	180	Eliminar y permitir recuperación
Eliminar después de un año	Etiqueta personal	365	Eliminar y permitir recuperación
Eliminar después de cinco años	Etiqueta personal	1.825	Eliminar y permitir recuperación
No eliminar nunca	Etiqueta personal	No aplicable	Eliminar y permitir recuperación

Nota: Para más información sobre etiquetas de retención consulte el siguiente enlace: https://docs.microsoft.com/es-es/exchange/policy-and-compliance/mrm/retention-tags-and-retention-policies?view=exchserver-2016

7.4 EXHIBICIÓN DE DOCUMENTOS ELECTRÓNICOS EN CONTEXTO

Una de las funcionalidades que más utilizan las organizaciones a la hora de investigar posibles casos de litigio es la exhibición de documentos electrónicos en contexto, lo que anteriormente se conocía como descubrimiento electrónico (eDiscovery).

Esta funcionalidad permite realizar búsquedas en uno o múltiples buzones (incluso en toda la organización) utilizando criterios como fechas, palabras clave, remitentes, destinatarios o tipos de elementos.

Como novedad, la exhibición de documentos electrónicos en contexto permite que, en el mismo proceso de búsqueda, se establezcan los buzones afectados en conservación local (In-Place Hold).

El control de acceso basado en roles proporciona el grupo de roles de administración de "Discovery Management" para delegar tareas de exhibición de documentos electrónicos en contexto a personal no técnico, sin necesidad de suministrar privilegios elevados que permitan a un usuario realizar cambios operativos en la configuración de Exchange.

Para que los usuarios realicen búsquedas de exhibición de documentos electrónicos en contexto, deben agregarse al grupo de roles de RBAC de "Discovery Management". Este grupo de roles consta de dos roles de administración: el rol búsqueda en el buzón, que permite a un usuario realizar una búsqueda de detección, y el rol retención legal, que permite a un usuario colocar un buzón de correo en retención por juicio o conservación local.

De forma predeterminada, el grupo de roles "Discovery Management" no tiene ningún miembro. Los permisos necesarios para realizar tareas relacionadas con la detección no se asignan a ningún usuario.

Además, de forma predeterminada, los administradores de Exchange no tienen permisos para realizar búsquedas de detección. Los administradores de Exchange que son miembros del grupo de roles de administración "Administración de la organización", pueden agregar usuarios al grupo de roles "Discovery Management" y crear grupos de roles personalizados para restringir el ámbito de un administrador de detección a un subconjunto de usuarios.

La auditoría de los cambios de roles de RBAC garantiza que se conserven los registros adecuados para realizar un seguimiento de la asignación del grupo de roles de "Discovery Management".

Al realizar una búsqueda de detección, debe especificarse un buzón de correo de destino donde almacenar los resultados de la búsqueda. Un buzón de detección es un tipo especial de buzón de Exchange 2016 que ofrece la siguiente funcionalidad:

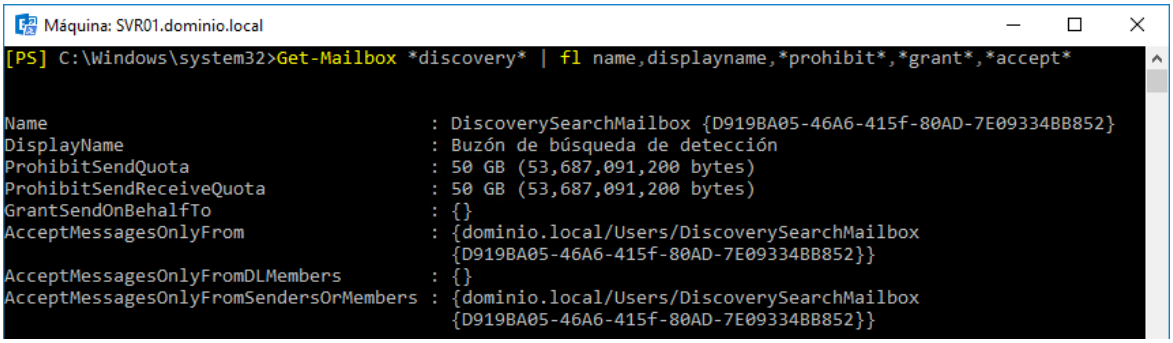
a) **Selección de buzón de correo de destino más simple y seguro.** Cuando se usa la consola Web de administración de Exchange para crear una búsqueda de detección, solo los buzones de correo de detección estarán disponibles como un repositorio donde almacenar los resultados de la búsqueda. No necesita revisar una posible lista extensa de buzones disponibles en la organización. Esto también elimina la posibilidad de que un administrador de detección seleccione accidentalmente otro buzón de correo del usuario o un buzón de correo no protegido donde almacenar contenido de mensajería potencialmente confidencial.

b) **Cuota de almacenamiento en buzones elevada.** El buzón de correo de destino debe poder almacenar la gran cantidad de mensajes que puede generar una búsqueda de detección. De forma predeterminada, los buzones de correo de detección tienen una cuota de almacenamiento de buzones de 50 gigabytes (GB). Puede modificarse la cuota según sus requisitos.

c) **Seguro de forma predeterminada.** Como todos los tipos de buzones, un buzón de detección posee una cuenta de usuario de Directorio Activo asociada. Sin embargo, esta cuenta está deshabilitada de forma predeterminada. Solamente los usuarios explícitamente autorizados para tener acceso al buzón de correo de detección tienen acceso al mismo. Los miembros del grupo de roles "Discovery Management" disponen de permiso de acceso total al buzón de detección predeterminado, sin embargo, los buzones de detección adicionales que pudieran crear no tienen asignado ningún permiso de acceso.

d) **Entrega de correo electrónico deshabilitada.** Si bien se puede ver en las listas de direcciones de Exchange, los usuarios no pueden enviar correo electrónico a un buzón de detección. La entrega de correo electrónico a los buzones de detección está prohibida por restricciones de entrega. Esto conserva la integridad de los resultados de búsqueda.

El programa de instalación de Exchange 2016 crea un buzón de detección con el nombre "Discovery Search Mailbox". Se puede utilizar el Shell para crear más buzones de correo de detección adicionales. De forma predeterminada, los buzones de correo de detección adicionales que se crean no tienen ningún permiso de acceso al buzón de correo asignado.



La búsqueda en varios buzones de correo también usa un buzón del sistema con el nombre "SystemMailbox {e0dc1c29-89c3-4034-b678-e6c29d823ed9}" para almacenar los metadatos de la búsqueda en varios buzones. Los buzones del sistema no se pueden ver en la consola Web de administración de Exchange ni en las listas de direcciones de Exchange.

Además, antes de poder eliminar una base de datos de buzones de correo donde está ubicado el buzón del sistema de la búsqueda en varios buzones, se debe mover el buzón a otra base de datos de buzones de correo.

El asistente para la suspensión y exhibición de documentos electrónicos local de la consola Web de administración de Exchange permite crear una búsqueda de exhibición de documentos electrónicos local y usar la retención local para retener los resultados de la búsqueda.

Al crear una búsqueda de exhibición de documentos electrónicos local, se crea un objeto de búsqueda en el buzón del sistema de exhibición de documentos electrónicos local. El objeto se puede manipular para iniciar, detener, modificar o quitar la búsqueda. Después de crear la búsqueda, puede optar por obtener una estimación de los resultados de la búsqueda, que incluye las estadísticas de palabras clave que le ayudarán a determinar la efectividad de la consulta.

También se puede obtener una vista previa dinámica de los elementos devueltos en la búsqueda, lo que permite ver el contenido de los mensajes, estimar el número de mensajes devueltos de cada buzón de origen y el número total de mensajes. Se puede utilizar esta información para ajustar aún más la consulta si fuera necesario.

La estimación incluye el número de elementos devueltos y su tamaño total. También se puede ver las estadísticas de palabras clave, que muestran detalles sobre el número de elementos devueltos para cada palabra clave que se usó en la consulta de búsqueda. Esta información resulta útil para determinar la efectividad de la consulta. Si la consulta es demasiado amplia, se devolverá un conjunto de datos mucho mayor, lo que requiere revisar más recursos y podría aumentar los costes de exhibición de documentos electrónicos. Si la consulta es demasiado limitada, podría reducir considerablemente el número de registros devueltos o no devolver ninguno.

Al crear una búsqueda de exhibición de documentos electrónicos, se deben especificar los siguientes parámetros:

a) Nombre. Corresponde al nombre de la búsqueda que se utilizará para identificarla. Al copiar los resultados de la búsqueda en un buzón de detección, se crea una carpeta en el buzón de detección con el nombre de la búsqueda y la marca de tiempo para identificar los resultados de la búsqueda de manera exclusiva en un buzón de detección.

b) Buzones de correo. Se puede elegir entre buscar en todos los buzones de la organización Exchange o especificar aquellos en los que se desee buscar. Tanto el buzón principal como el buzón de archivo de un usuario se incluyen en la búsqueda. Asimismo, si se desea usar la misma búsqueda para retener elementos, se debe especificar los buzones. Se puede hacer uso de un grupo de distribución para incluir usuarios de buzones de correo que sean miembros de ese grupo, aunque hay que tener en cuenta que la pertenencia al grupo se calcula una vez creada la búsqueda y los cambios posteriores en la pertenencia al grupo no se reflejan de manera automática en la búsqueda.

c) Palabras clave. Se pueden especificar palabras clave y frases para buscar contenidos en los mensajes. También se pueden utilizar los operadores lógicos AND, OR o NOT y, de manera adicional, Exchange Server 2016 también admite el operador NEAR, que permite buscar una palabra o frase que esté cerca de otras. Para buscar una coincidencia exacta de una frase de varias palabras, debe colocar la frase entre comillas. Exchange Server 2016 también admite la sintaxis del lenguaje de consulta de palabras clave (KQL) para las búsquedas de exhibición de documentos electrónicos local, aunque no se admiten expresiones regulares. Por último, los operadores lógicos deben estar en mayúsculas como, por ejemplo, AND y OR, para que se traten como operadores en lugar de palabras clave. Se recomienda usar paréntesis explícitos en las consultas donde se mezclen varios operadores lógicos para evitar errores o malas interpretaciones.

d) Fechas de inicio y de finalización. De forma predeterminada, la exhibición de documentos electrónicos no limita las búsquedas por intervalos de fechas. Para buscar mensajes enviados durante un intervalo de fechas específico, se puede limitar la búsqueda especificando la fecha de inicio y de finalización. Si no se especifica una fecha de finalización, la búsqueda mostrará los últimos resultados cada vez que se reinicie la búsqueda.

e) Remitentes y destinatarios. Para limitar la búsqueda, se pueden especificar los remitentes y los destinatarios de los mensajes. Para ello, se puede utilizar direcciones de correo electrónico, nombres para mostrar o el nombre de un dominio para buscar los elementos que ha enviado alguien o que se han enviado a alguien en el dominio.

f) Tipos de mensajes. De forma predeterminada, se realizan búsquedas en todos los tipos de mensaje. Para limitar la búsqueda, se puede seleccionar diferentes tipos de mensajes como correo electrónico, contactos, documentos, diario, reuniones, notas o contenido de Lync.

g) Datos adjuntos. La exhibición de documentos electrónicos busca datos adjuntos que sean compatibles con Exchange Search como ficheros de Microsoft Office, PDF, imágenes u otros. Así mismo, se puede agregar compatibilidad con tipos de archivos adicionales al instalar filtros de búsqueda (también conocidos como iFilter) para el tipo de archivo que hay en los servidores de buzones de correo.

h) Elementos que no permiten búsquedas. Los elementos en los que no se puede buscar son los elementos de los buzones que Exchange Search no puede indizar. Entre los motivos por los que no se pueden indizar se incluye la falta de un filtro de búsqueda instalado para un dato adjunto, un error de filtro o mensajes cifrados. Para que una búsqueda de exhibición de documentos electrónicos se realice correctamente, puede que se le solicite a la organización que incluya dichos elementos para que se revisen. Al copiar los resultados de la búsqueda a un buzón de detección o al exportarlos a un archivo PST, puede incluir elementos no aptos para la búsqueda.

i) Elementos cifrados. Como Exchange Search no puede indizar los mensajes cifrados con S/MIME, la exhibición de documentos electrónicos no realiza búsquedas en estos mensajes. Si se selecciona la opción para incluir los elementos que no permiten búsquedas en los resultados de la búsqueda, estos mensajes cifrados con S/MIME se copian tal cual en el buzón de detección. Posteriormente se requerirá la calve privada del certificado S/MIME para descifrar el contenido del elemento.

j) Elementos protegidos por IRM. Exchange Search puede indizar los mensajes protegidos con "Information Rights Management (IRM)" y, por lo tanto, se incluyen en los resultados de la búsqueda sí coinciden con los parámetros de consulta. Los mensajes deben haberse protegido mediante un servicio Active Directory Rights Management Services (AD RMS) situado en el mismo bosque de Directorio Activo que el servidor de buzones de correo.

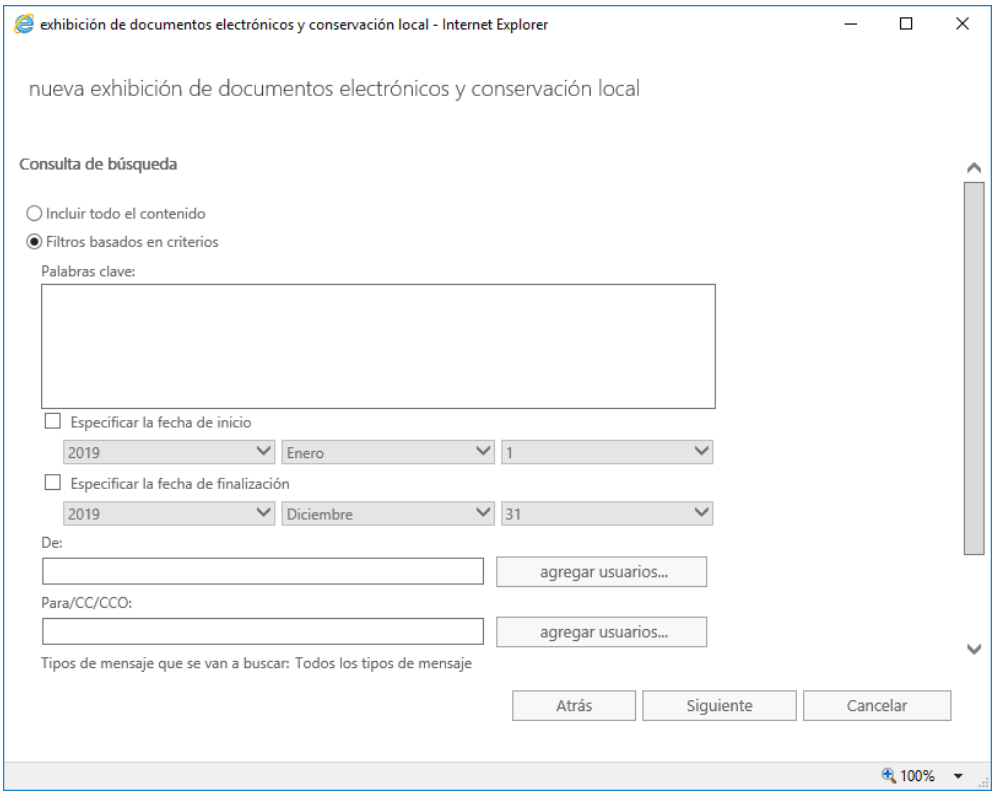
Nota: Cuando Exchange Search no puede indizar un mensaje protegido por IRM, ya sea por un error de descifrado o porque IRM está deshabilitado, el mensaje protegido no se agrega a la lista de elementos en los que se ha producido un error. Si se selecciona la opción para incluir los elementos que no permiten búsquedas en los resultados de la búsqueda, es posible que los resultados no incluyan los mensajes protegidos por IRM que no se pudieron descifrar, por lo tanto, para incluir los mensajes protegidos por IRM en la búsqueda, se puede crear otra búsqueda que incluyan los mensajes con datos adjuntos ".rpmsg". Se puede utilizar la cadena de consulta "attachment:rpmsg" para buscar mensajes protegidos por IRM en los buzones especificados, independientemente de si están indizados correctamente o no.

k) Desduplicación. Al copiar los resultados de la búsqueda en un buzón de detección, se puede habilitar la desduplicación de los resultados de la búsqueda para copiar solo una instancia de un único mensaje en el buzón de detección. La desduplicación tiene las siguientes ventajas:

   i. Requisitos de almacenamiento y tamaño de buzón de detección menores debido a la disminución de la cantidad de mensajes copiados.

   ii. Reducción de la carga de trabajo para los administradores de detección, los asesores legales o cualquier otro individuo que esté involucrado en la revisión de los resultados de la búsqueda.

   iii. Reducción del coste de la exhibición de documentos electrónicos, en función del número de elementos duplicados de los resultados de la búsqueda.



Adicionalmente, Exchange Server 2016 permite crear un registro de las búsquedas realizadas, por cuestiones de seguridad. Para ello, existen dos tipos de registro disponibles en las búsquedas de detección:

a) **Registro básico.** El registro básico está habilitado de forma predeterminada para todas las búsquedas de exhibición de documentos electrónicos. Este tipo de registro incluye información acerca de la búsqueda y quién la realizó. La información que captura el registro básico se muestra en el mensaje de correo electrónico que se envía al buzón de correo en el que se almacenan los resultados de la búsqueda. El mensaje se encuentra en la carpeta que se crea para almacenar los resultados de la búsqueda.

b) **Registro completo.** El registro completo incluye información acerca de todos los mensajes que muestra la búsqueda. Esta información se proporciona en un archivo con formato de valores separados por comas (.csv) que se adjunta al mensaje de correo electrónico que contiene la información del registro básico. El nombre de la búsqueda se usa para generar el nombre del archivo ".csv". Esta información puede ser necesaria para el cumplimiento de normas o la conservación de un registro. Para habilitar el registro completo, seleccione la opción **Habilitar el registro completo** al copiar los resultados de búsqueda a un buzón de correo de detección en el EAC. Si se utiliza el Shell, se puede especificar la opción de registro completo mediante el parámetro "LogLevel".

Nota: Además del registro de búsqueda incluido al copiar los resultados de la búsqueda en un buzón de detección, Exchange Server 2016 también registra los cmdlets que usa el EAC o el Shell para crear, modificar o quitar búsquedas de exhibición de documentos electrónicos local. Esta información se registra en las entradas del registro de auditoría de administración.

Una vez copiados los resultados de la búsqueda a un buzón de detección, se puede exportar dicho contenido a un archivo PST y de esta forma, abrir el archivo en Outlook para su revisión posterior o la impresión de los mensajes relevantes.

7.5 CONSERVACIÓN LOCAL Y RETENCIÓN POR JUICIO

Cuando existen sospechas sobre posibles litigios o incidentes de seguridad o vulneración de la confidencialidad, se puede solicitar a una organización que conserve toda la información almacenada electrónicamente (incluido el correo electrónico) que sea relevante para el caso.

Dichas sospechas pueden tener lugar antes de que se conozcan los pormenores del caso, por lo que se suele conservar gran cantidad de material. Las organizaciones pueden conservar todo el correo electrónico relacionado con un tema concreto o el perteneciente a ciertos usuarios.

En función de los procesos de detección electrónica de la organización, algunas de las medidas que se pueden adoptar para conservar el correo electrónico son:

a) Pedir a los usuarios finales que no eliminen ningún mensaje para conservar el correo electrónico. No obstante, los usuarios podrían eliminar igualmente correo electrónico de forma intencionada o sin darse cuenta.

b) Suspender los mecanismos de eliminación automatizados como, por ejemplo, la administración de registros de mensajes (MRM). Esta medida podría generar una acumulación excesiva de correo electrónico en el buzón de correo del usuario y afectar negativamente a su productividad. Además, el hecho de suspender la eliminación automatizada no impide que los usuarios eliminen manualmente el correo electrónico.

c) Copiar o mover el correo electrónico a un archivo para asegurarse de que no se elimina ni altera ni manipula. Esta medida incrementa el coste de mantenimiento porque es necesario copiar o mover los mensajes de forma manual a un archivo, o a productos de terceros utilizados para reunir y almacenar el correo electrónico fuera de Microsoft Exchange.

Así mismo, si el correo electrónico no se conserva, la organización puede quedar expuesta a riesgos legales o financieros, como la inspección de procesos de detección y conservación de datos, sentencias judiciales adversas, sanciones o multas.

Es por ello que Exchange Server 2016 ofrece herramientas para conservar la información de forma sencilla y sin afectar al trabajo diario del usuario o usuarios afectados por el litigio, permitiendo cumplir con los siguientes objetivos:

a) Establecer los buzones de los usuarios en retención y conservar los elementos del buzón inmutablemente.

b) Preservar los elementos de buzón eliminados por los usuarios o por procesos de supresión automática como MRM.

c) Conservar mensajes que se reenvían a otro buzón de correo.

d) Usar la retención local basada en consultas para buscar y conservar elementos que coincidan con criterios especificados.

e) Conservar elementos indefinidamente o durante un tiempo concreto.

f) Marcar un usuario en varias suspensiones en función de investigaciones o casos distintos.

g) Mantener activa la administración MRM de modo que las retenciones resulten transparentes para el usuario.

h) Habilitar búsquedas de la exhibición de documentos electrónicos de elementos en retención.

En la versión de Exchange Server 2010, el término "retención legal" se entendía como el proceso para mantener todos los datos del buzón de correo de un usuario de forma indefinida o hasta que cuando se eliminara la suspensión. En Exchange 2016, al igual que en 2013, la conservación local ha introducido un modelo diferente que permite especificar parámetros adicionales a la retención:

a) **Retención basada en consulta:** con la suspensión por litigio, se conservan todos los elementos de un buzón de correo. Sin embargo, una retención local permite especificar qué elementos retener para contener mediante el uso de parámetros de consulta de búsqueda (como palabras clave, remitentes, destinatarios, iniciar y finalizar fechas) y también especificar los tipos de mensajes (como mensajes de correo electrónico, los elementos de calendario y las conversaciones de Skype para la empresa que desee poner en espera). Después de crear una consulta basada en conservación local, se conservan todos los elementos existentes y elementos de buzón futuros (incluidos los mensajes recibidos en una fecha posterior) que coinciden con los parámetros de consulta. La suspensión por litigio no admite suspensiones basada en consultas.

b) **Duración de la retención:** en juicio y conservación local, se puede especificar cuánto tiempo se contienen los elementos. Se puede especificar una duración de retención infinita o una duración de retención basada en tiempo. La duración se calcula a partir de la fecha de un elemento de buzón de correo se ha recibido o creado. Por ejemplo, si la organización requiere que todos los elementos del buzón de correo se conserven durante siete años, puede crear una retención basada en tiempo. Por lo que, si un buzón de correo se pone en espera y la duración de retención se establece en 7 años, el elemento en el buzón de correo se elimina permanentemente después de 2 años a partir de la fecha que se recibió y se mantiene 5 años antes de purgarse desde la base de datos del buzón de correo.

Los usuarios autorizados que se hayan agregado al grupo de roles de control de acceso basado en roles (RBAC) de administración de la detección o se les hayan asignado los roles de administración de la retención legal y búsqueda de buzón pueden marcar a los usuarios en conservación local. Esta tarea se puede delegar en administradores de registros, responsables de cumplimiento normativo o abogados del departamento jurídico de la organización, a la vez que se asigna el menor número de privilegios posible.

En Exchange 2013, el rol de retención legal proporcionaba permisos suficientes a un usuario para poner los buzones en retención por juicio. En Exchange 2016, puede usar los mismos permisos para colocar buzones de correo en una conservación local indefinida o basada en tiempo. No obstante, para crear una retención local basada en consulta, el usuario tiene que tener asignado el rol de búsqueda de buzones. El grupo de roles "Discovery Management" tiene ambos roles asignados.

La conservación local y la retención por juicio usan la carpeta de elementos recuperables para conservar los elementos. Esta carpeta sustituye la característica conocida como contenedor en las versiones anteriores de Exchange. La carpeta de elementos recuperables está oculta en la vista predeterminada de Outlook, Outlook en la Web y otros clientes de correo electrónico.

De manera predeterminada, cuando un usuario elimina un mensaje de una carpeta que no es la carpeta de elementos eliminados, dicho mensaje se mueve a esta última. Esto se denomina movimiento. Cuando un usuario elimina temporalmente un elemento (para lo cual debe presionar las teclas MAYÚS y SUPR) o lo elimina de la carpeta de elementos eliminados, el mensaje se mueve a la carpeta de elementos recuperables, por lo que desaparece de la vista del usuario.

Los elementos de la carpeta elementos recuperables se conservan durante el periodo de retención de elementos eliminados que está configurado en la base de datos de buzones de correo del usuario.

De manera predeterminada, dicho periodo está establecido en 14 días para las bases de datos de buzones de correo. También se puede configurar una cuota de almacenamiento para la carpeta elementos recuperables. Así, la organización queda protegida ante un posible ataque por denegación de servicio (DoS) debido al rápido crecimiento de la carpeta de elementos recuperables y, por tanto, de la base de datos de buzones de correo.

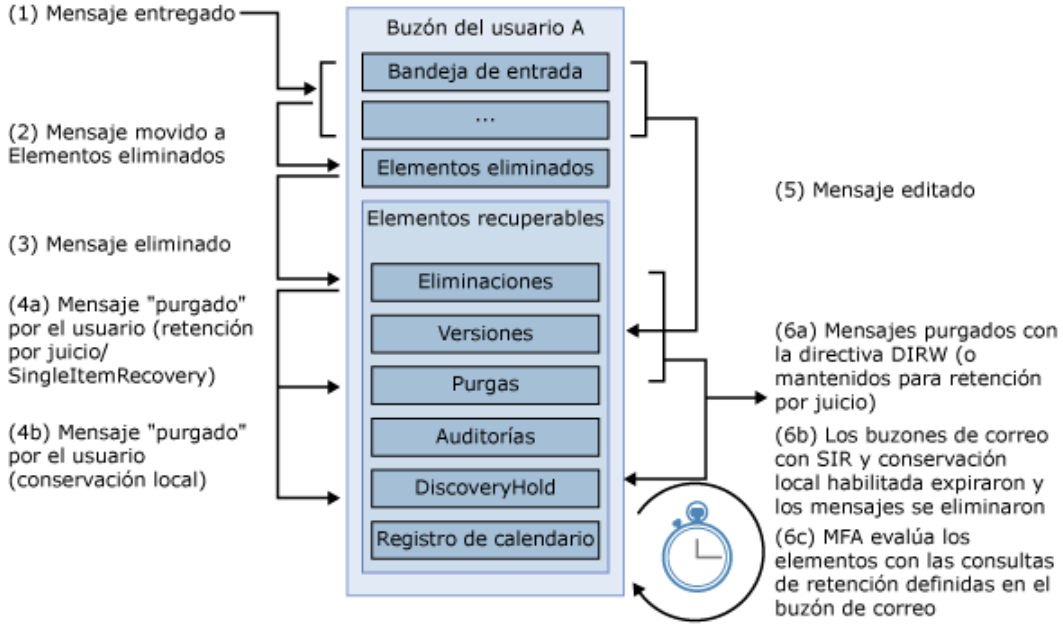
Si un buzón de correo no se pone en conservación local o en retención por juicio, los elementos se eliminan permanentemente de la carpeta de elementos recuperables por el procedimiento "primero en entrar, primero en salir" siempre que se exceda la cuota de advertencia de dicha carpeta o si el elemento ha permanecido en la carpeta más tiempo del que establece el período de retención de elementos eliminados. La carpeta Elementos recuperables contiene las subcarpetas siguientes, que se usan para almacenar los elementos eliminados en distintos sitios y facilitar la conservación local y la retención por juicio:

a) Deletions. Los elementos quitados de la carpeta de elementos eliminados o los eliminados temporalmente de otras carpetas se mueven a la subcarpeta eliminaciones, donde el usuario los puede ver con la característica "Recuperar elementos eliminados de Outlook y Outlook en la Web". De forma predeterminada, los elementos permanecen en esta carpeta hasta que finaliza el periodo de retención de elementos eliminados que se ha configurado para la base de datos de buzones de correo o hasta que el buzón caduque.

b) Purges. Cuando un usuario elimina un elemento de la carpeta de elementos recuperables, el elemento se mueve a la carpeta "Purges", de igual forma, los elementos que superan el periodo de retención de elementos eliminados configurado en la base de datos de buzones de correo o en el buzón también se mueven a esta carpeta. Los usuarios no pueden ver los elementos de esta carpeta, aunque utilicen la herramienta recuperar elementos eliminados. Cuando el asistente de buzones de correo procesa el buzón de correo, los elementos de esta carpeta se eliminan de la base de datos de buzones de correos. Sin embargo, al poner al buzón del usuario en retención por juicio, el asistente de buzones no elimina los elementos de esta carpeta.

c) DiscoveryHold. Si un usuario se marca en conservación local, los elementos eliminados se desplazan a esta carpeta. Cuando el asistente del buzón procesa el buzón de correo, analiza los mensajes de esta carpeta y los elementos que coinciden con la consulta de retención local se retienen hasta el período de retención especificado en la consulta. Si no se especifica un período de retención, los elementos se conservarán indefinidamente o hasta que se quite la retención del usuario.

d) Versions. Cuando un usuario se pone en conservación local o en retención por juicio, los elementos del buzón deben estar protegidos de cualquier manipulación o modificación por parte del usuario o de un proceso. Esto se consigue mediante el proceso protección de página de escritura en copia (copy-on-write), el cual, cuando un usuario o proceso modifican las propiedades concretas de un elemento del buzón de correo, se guarda una copia del elemento original en la carpeta de versiones antes de que se confirme el cambio. El proceso se repite para todos los cambios posteriores. Los elementos contenidos en la carpeta versiones también se indexan y se devuelven en las búsquedas de la exhibición de documentos electrónicos local. Después de quitar la retención, el asistente para carpeta administrada elimina las copias de la carpeta versiones.



7.6 REGISTRO DE AUDITORÍA DE BUZÓN

Otra de las herramientas que proporciona Exchange Server 2016 para controlar y auditar posibles accesos no autorizados a buzones sensibles de la organización es el registro de auditoría de buzón.

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. De forma predeterminada no se registra ninguna de las acciones realizadas por el propietario del buzón.

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

Las entradas del registro se almacenan en la carpeta de elementos recuperables en el buzón auditado, en la subcarpeta "Auditorías". Esto garantiza que las entradas del registro de auditoría estén disponibles en una ubicación única, independientemente del método de acceso del cliente que se haya usado para acceder al buzón o del servidor o estación de trabajo que un administrador haya usado para acceder al registro de auditoría de buzón.

Así mismo, si se mueve un buzón de correo a otro servidor de buzones de correo, también se moverán los registros de auditoría de buzón pertinentes porque se encuentran en el mismo buzón de correo.

De forma predeterminada, las entradas de un registro de auditoría de buzón se conservan en el buzón de correo durante 90 días y luego se eliminan. Puede modificar este período de retención con el parámetro "AuditLogAgeLimit" del cmdlet "Set-Mailbox".

Al habilitar el registro de auditoría para un buzón de correo, se puede especificar qué acciones de usuario (por ejemplo, obtener acceso a un mensaje, moverlo o eliminarlo) se deben registrar para un tipo de inicio de sesión (administrador, usuario delegado o propietario) determinado.

Las entradas del registro de auditoría también incluyen información importante, como la dirección IP del cliente, el nombre de host y el proceso o el cliente usado para obtener acceso al buzón de correo. Para los elementos movidos, la entrada incluye el nombre de la carpeta de destino.

El registro de auditoría de buzón se habilita por buzón de correo. El cmdlet "Set-Mailbox" permite habilitar o deshabilitar el registro de auditoría de buzón. Al habilitar el registro de auditoría de buzón en un buzón, el acceso al buzón de correo y algunas acciones realizadas por los administradores y delegados se registran de forma predeterminada. Para registrar las acciones que lleva a cabo el propietario del buzón, es necesario especificar las acciones de propietario que se deben auditar.

En la siguiente tabla se enumeran las acciones registradas por el registro de auditoría de buzón de correo, incluidos los tipos de inicio de sesión para los que se puede registrar la acción.

Acción	Descripción	Administrador	Delegado	Propietario
Copiar	Se copia un elemento en otra carpeta.	Sí	No	No
Create	Se crea un elemento en la carpeta Calendario, Contactos, Notas o Tareas en el buzón. Por ejemplo, se crea una nueva convocatoria de reunión. Tenga en cuenta que la creación de carpetas o mensajes no se audita.	Sí*	Sí*	Sí
FolderBind	Se obtiene acceso a una carpeta de buzón de correo.	Sí*	Sí**	No
HardDelete	Se elimina un elemento de la carpeta Elementos recuperables de forma permanente.	Sí*	Sí*	Sí
MailboxLogin	El usuario inició sesión en su buzón.	No	No	Sí***
MessageBind	Se abre o se obtiene acceso a un elemento desde el panel de lectura.	Sí	No	No
Mover	Se mueve un elemento a otra carpeta.	Sí*	Sí	Sí
MoveTo DeletedItems	Se mueve un elemento a la carpeta Elementos eliminados.	Sí*	Sí	Sí
SendAs	Se envía un mensaje con los permisos Enviar como.	Sí*	Sí*	No aplicable

Acción	Descripción	Administrador	Delegado	Propietario
SendOn Behalf	Se envía un mensaje con los permisos Enviar en nombre de.	Sí*	Sí	No aplicable
SoftDelete	Se elimina un elemento de la carpeta Elementos eliminados.	Sí*	Sí*	Sí
Actualizar	Se actualizan las propiedades de un elemento.	Sí*	Sí*	Sí

Nota: *Se audita de forma predeterminada si la auditoría está habilitada para el buzón en cuestión. **Se consolidan las entradas de las acciones de enlace de carpeta realizadas por delegados. Se genera una entrada de registro para el acceso a cada carpeta en un plazo de 24 horas. Auditoría de *** para inicios de sesión de propietario a un buzón de correo sólo funciona para los inicios de sesión de POP3, IMAP4 o OAuth. No funciona para los inicios de sesión NTLM o Kerberos para el buzón de correo.

Se pueden utilizar deferentes métodos para buscar entradas en el registro de auditoría de buzón:

a) **Buscar en un único buzón de forma sincrónica.** Mediante el cmdlet "Search-MailboxAuditLog" se puede buscar de forma sincrónica las entradas de registro de auditoría de buzón en un único buzón de correo. El cmdlet muestra los resultados de la búsqueda en la ventana del Shell de administración de Exchange.

b) **Buscar en uno o más buzones de forma asincrónica.** Se puede crear una búsqueda de registros de auditoría de buzón mediante el cmdlet "New-MailboxAuditLogSearch" para buscar de forma asincrónica en uno o más buzones de correo y, a continuación, enviar los resultados de la búsqueda a una dirección de correo electrónico especificada. Los resultados de la búsqueda se envían como datos adjuntos XML. Para crear la búsqueda, use.

c) **Usar informes de auditoría en el Centro de administración de Exchange (EAC).** puede usar la pestaña auditoría en el EAC para ejecutar un informe de acceso al buzón de correo del que no se es propietario o para exportar entradas del registro de auditoría de buzón.

En la tabla siguiente se describen los campos registrados en una entrada de registro de auditoría de buzón.

Campo	Se rellena con
Operation	Una de las acciones siguientes: – Copiar – Create – FolderBind – HardDelete – MessageBind – Mover – MoveToDeletedItems – SendAs – SendOnBehalf – SoftDelete – Actualizar
OperationResult	Uno de los resultados siguientes: – Failed – PartiallySucceeded – Succeeded
LogonType	Tipo de inicio de sesión del usuario que realizó la operación. Entre los tipos de inicio de sesión, se incluyen: – Propietario – Delegado – Admin
DestFolderId	GUID de la carpeta de destino para las operaciones de movimiento.
DestFolderPathName	Ruta de acceso de la carpeta de destino para las operaciones de movimiento.
FolderId	GUID de la carpeta.
FolderPathName	Ruta de acceso de la carpeta.
ClientInfoString	Detalles que identifican qué cliente o qué componente de Exchange realizó la operación.
ClientIPAddress	Dirección IP del equipo cliente.
ClientMachineName	Nombre del equipo cliente.
ClientProcessName	Nombre del proceso de la aplicación cliente.
ClientVersion	Versión de la aplicación cliente.
InternalLogonType	Tipo de inicio de sesión del usuario que realizó la operación. Entre los tipos de inicio de sesión, se incluyen: – Propietario – Delegado – Admin
MailboxOwnerUPN	Nombre principal de usuario (UPN) del propietario del buzón.
MailboxOwnerSid	Identificador de seguridad del propietario del buzón (SID).
DestMailboxOwnerUPN	Nombre principal de usuario (UPN) del propietario del buzón de destino, registrado para operaciones entre buzones.
DestMailboxOwnerSid	SID del propietario del buzón de destino, registrado para operaciones entre buzones.

Campo	Se rellena con
DestMailboxOwnerGuid	GUID del propietario del buzón de destino.
CrossMailboxOperation	Información sobre si la operación registrada es una operación entre buzones (por ejemplo, copiar o mover mensajes entre buzones).
LogonUserDisplayName	Nombre para mostrar del usuario que ha iniciado sesión.
DelegateUserDisplayName	Nombre para mostrar del usuario delegado.
LogonUserSid	SID del usuario que ha iniciado sesión.
SourceItems	Identificador de elemento de los elementos de buzón donde se haya realizado la acción registrada (por ejemplo, mover o eliminar). Para las operaciones realizadas en varios elementos, este campo se devuelve como un conjunto de elementos.
SourceFolders	GUID de la carpeta de origen.
ItemId	Identificador del elemento.
ItemSubject	Asunto del elemento.
MailboxGuid	GUID del buzón.
MailboxResolvedOwnerName	Nombre resuelto del usuario de buzón con el formato DOMINIO\NombreCuentaSam.
LastAccessed	Hora en que se realizó la operación.
Identity	Identificador de entrada de registro de auditoría.

7.7 CLASIFICACIÓN DE MENSAJES

Las clasificaciones de mensajes son una característica de Microsoft Exchange Server y de Microsoft Office Outlook, destinada a ayudar a las organizaciones a cumplir sus directivas de correo y sus responsabilidades normativas.

Cuando un mensaje está clasificado, significa que contiene metadatos específicos que describen el uso o el público al que se destina el mensaje. Outlook o Microsoft Office Outlook en la Web pueden actuar sobre estos metadatos al mostrar una descripción sencilla de la clasificación a los remitentes y los destinatarios de un mensaje clasificado.

En Exchange Server 2016, el servicio de transporte puede responder ante estos metadatos si existe una regla de transporte que cumpla los criterios específicos que se han configurado. La lista siguiente proporciona una descripción breve de algunos de los campos de clasificación de mensajes que puede establecer:

a) Nombre para mostrar. Esta propiedad especifica el nombre para mostrar para la instancia de clasificación de mensaje. Este nombre para mostrar aparece en el menú permiso en Outlook y Outlook en la Web y lo pueden utilizar los usuarios de Outlook y de Outlook en la Web para seleccionar la clasificación de mensaje adecuada antes de enviar un mensaje. El nombre para mostrar también se muestra en la descripción del destinatario que aparece en la barra de información en un mensaje de Outlook. El nombre de parámetro de esta propiedad es “DisplayName”.

b) Descripción del remitente. Esta propiedad explica al remitente cuál es el objetivo de la clasificación de mensaje. Los usuarios de Outlook y de Outlook en la Web pueden utilizar el texto que se especifique en este campo para seleccionar la clasificación de mensajes adecuada antes de enviar un mensaje. El nombre de parámetro de esta propiedad es "SenderDescription".

c) Descripción del destinatario. Esta propiedad explica al destinatario cuál es el objetivo de la clasificación de mensaje. Los usuarios de Outlook y de Outlook en la Web visualizan el texto que se especifique en este campo al recibir un mensaje que tenga esta clasificación de mensajes. El nombre de parámetro de esta propiedad es "RecipientDescription".

d) Configuración regional. Este campo especifica un código cultural para crear una versión específica de la configuración regional de la clasificación de mensajes. El nombre de parámetro de esta propiedad es "Locale".

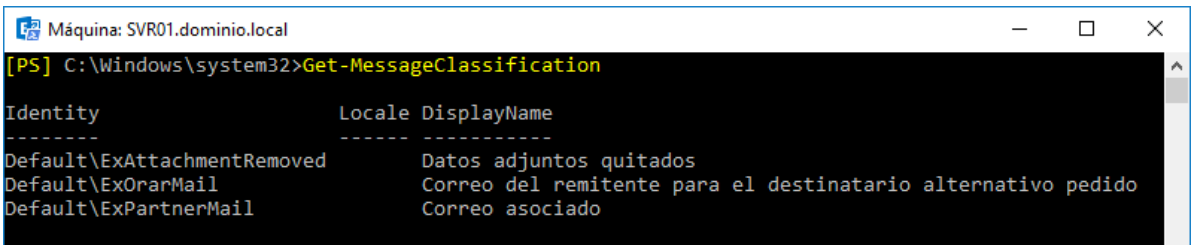
Después de habilitar Outlook para que acepte las clasificaciones de mensajes predeterminadas, los usuarios pueden aplicar la clasificación de mensajes a los mensajes que envíen. Los remitentes visualizan la descripción de remitente en la barra de información de Outlook. Mediante el Shell de administración de Exchange, se puede personalizar la descripción del remitente para cada clasificación de mensajes y configuración regional. Outlook en la Web no necesita una configuración especial para mostrar o usar clasificaciones de mensajes.

Hay tres clasificaciones de mensajes habilitadas de forma predeterminada en Exchange 2016:

a) Datos adjuntos quitados. Esta clasificación notifica a los remitentes cuando se quitaron datos adjuntos del mensaje.

b) Correo del remitente para el destinatario alternativo solicitado. Esta clasificación notifica a los destinatarios que el mensaje se redireccionó para la entrega al destinatario original.

c) Correo de asociado. Esta clasificación notifica a los destinatarios que el mensaje se cifró y entregó por medio de un conector seguro.



En la instalación inicial de Exchange Server 2016, todas las clasificaciones de mensajes son solo informativas. No están asociadas a ninguna regla de transporte y solamente proporcionan información adicional acerca de un mensaje a los destinatarios del mismo, por lo tanto, de forma predeterminada, en Exchange Server 2016, el servicio de transporte no realiza ninguna acción especial en el mensaje.

Sin embargo, se pueden crear reglas de transporte basadas en las clasificaciones de mensajes. Por ejemplo, se puede configurar una regla de transporte que compruebe una clasificación de mensajes específica para todos los mensajes entrantes e indique que esos mensajes se entreguen a un destinatario concreto.

Las clasificaciones de mensajes se pueden separar de forma lógica en dos clases, en función de cómo están relacionadas con un mensaje específico:

a) El remitente de un mensaje puede agregar una clasificación de mensaje de forma manual antes de enviar el mensaje.

b) Una clasificación de mensaje se puede agregar como resultado de la aplicación de una regla. Por ejemplo, cuando el agente de filtrado de datos adjuntos quita un adjunto de un mensaje, la clasificación de datos adjuntos quitados se agrega al mensaje. Cuando el destinatario recibe el mensaje, Outlook muestra una explicación de la razón por la cual se han quitado los datos adjuntos en la descripción de destinatario de la barra de información. Un administrador de Exchange puede personalizar la descripción del destinatario.

De forma predeterminada, una clasificación de mensaje viaja con un mensaje durante toda la vida del mensaje hasta que sale de la organización. Por lo tanto, si un remitente envía una clasificación de mensaje en un mensaje específico, éste conservará la clasificación de mensaje siempre que otras reglas no la eliminen.

A cada clasificación de mensaje se le puede asignar una prioridad relativa a otras clasificaciones de mensaje. Esto configura la precedencia en una clasificación determinada y cómo se muestra al destinatario en Outlook. Primero se muestra la clasificación de mensaje con mayor precedencia y, a continuación, se muestran en el orden adecuado las clasificaciones posteriores con menor grado de precedencia. Se puede configurar la preferencia mediante el parámetro "DisplayPrecedence" en el cmdlet "Set-MessageClassification" en el Shell.

Para cada clasificación de mensaje se puede especificar si la clasificación de mensaje se retiene cuando un destinatario responde a o reenvía el mensaje. Puede especificar si una clasificación se retiene al configurar el parámetro "RetainClassificationEnabled" en el cmdlet "Set-MessageClassification" del Shell.

Cuando se crea una clasificación de mensaje y se habilita el equipo en el que se ejecuta Outlook, la clasificación de mensaje nueva aparecerá en el menú permiso de Outlook y Outlook en la Web.

Así mismo, se puede controlar el acceso de lectura de las clasificaciones de mensaje incluidas en el menú permiso de Outlook si se configuran las clasificaciones de mensajes que se exportan al archivo "Classifications.xml".

Se puede controlar el acceso de lectura de las clasificaciones de mensaje si se configuran los permisos de lectura en el objeto de clasificación de mensaje. De manera predeterminada, todas las clasificaciones de mensajes se crean con permiso de lectura para cualquier usuario autenticado en el objeto de clasificación de mensaje en Directorio Activo.

Es importante comprender que los permisos de lectura que se establecen en el objeto de clasificación de mensaje no controlan si el remitente puede usar la clasificación de mensaje.

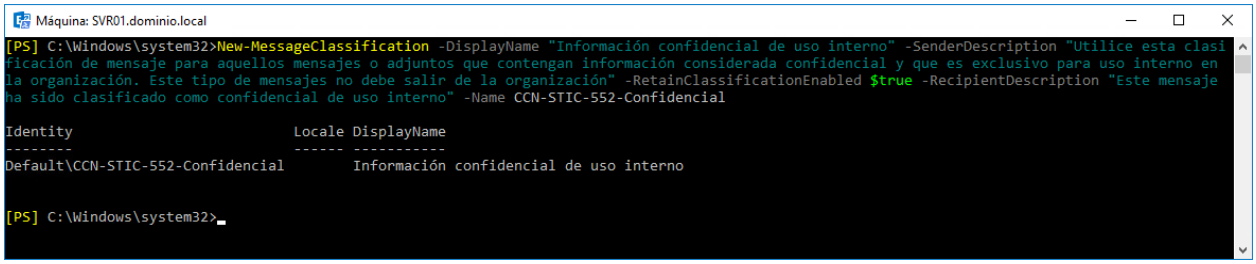
Los permisos de lectura de la clasificación de mensaje solo controlan si dicha clasificación se muestra en el menú permiso de Outlook en la Web. Los usuarios de Outlook pueden enviar clasificaciones de mensaje incluso si el usuario no tiene acceso de lectura a la clasificación de mensaje. Los usuarios avanzados tienen la posibilidad de enviar mensajes clasificados al editar el archivo Classifications.xml instalado en sus equipos para habilitar las clasificaciones de mensaje en Outlook.

Después de crear una instancia de clasificación de mensaje, es posible asociar una regla de transporte a dicha clasificación. Se usa el Shell para crear una regla de transporte y agregar la clasificación de mensaje como una condición.

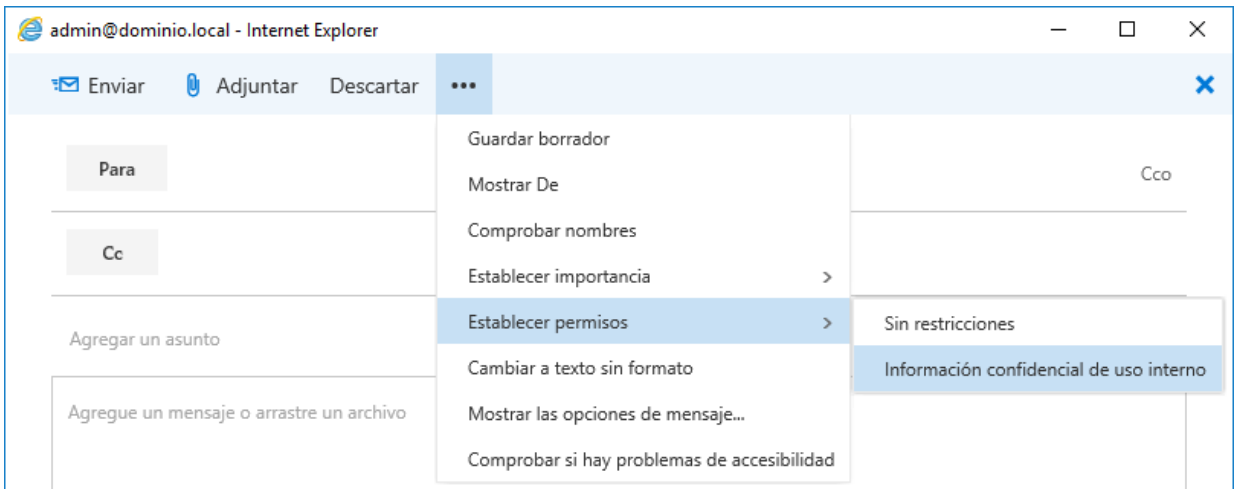
Antes de que los usuarios de Outlook puedan establecer y ver las clasificaciones de mensajes, deben instalar los archivos de configuración de clasificación de mensajes y crear una clave del Registro de Outlook en los equipos de los usuarios finales. Las plantillas de clasificación de mensajes de Outlook son archivos ".xml" que se deben generar después de crear y configurar las clasificaciones de mensajes.

Se pueden administrar todas las clasificaciones de mensaje con los cmdlets de clasificación de mensaje del Shell. Así mismo, se pueden enlazar clasificaciones de mensaje con reglas de transporte mediante el Shell o la Consola de administración de Exchange (EMC).

En la siguiente imagen se muestra la creación de una clasificación de mensajes para mensajes con carácter confidencial.



Una vez creada, automáticamente la clasificación de mensajes se muestra tanto en Outlook como en Outlook en la Web para que el usuario pueda hacer uso de dicha clasificación y que, opcionalmente, se le vincule una regla de transporte que realice alguna acción con el mensaje, como bloquear su envío fuera de la organización.



7.8 ARCHIVO LOCAL

Tal y como ya se ha mencionado anteriormente, cuando se hablaba de la administración de registros de mensajes (MRM), Exchange Server 2016 ofrece la posibilidad de habilitar un buzón de archivo a cada uno de los usuarios para almacenar información de uso poco frecuente en un contexto separado del buzón donde reside la bandeja de entrada.

Así mismo, mediante etiquetas de mensajes y reglas de administración de registros de mensajes, se pueden mover los mensajes que superen una cierta edad a dicho buzón de archivo local para su preservación durante un número determinado de años.

Uno de los grandes problemas para las organizaciones es la gestión que deben realizar de grandes cantidades de datos diseminados entre los equipos de los usuarios en formato de archivos ".pst".

Outlook usa archivos ".pst" para almacenar datos localmente en los equipos de los usuarios o los recursos compartidos de red. A diferencia de los archivos de almacén sin conexión (.ost) (que usa Outlook en el modo caché de Exchange para almacenar una copia del buzón de correo para acceso sin conexión), los archivos .pst no se sincronizan con el buzón de correo de Exchange del usuario. Si un usuario mueve mensajes a un archivo ".pst", dichos mensajes se quitan del buzón de correo.

El almacenamiento y el mantenimiento de mensajes antiguos supone un reto y un serio problema para las organizaciones, sobre todo en aspectos como:

a) El cumplimiento legal o normativo.

b) La administración de las copias de seguridad.

c) El control de acceso sobre la información.

Desde hace ya muchos años, se utilizan ficheros .pst de Outlook como repositorios de información antigua, pero que, en ningún caso, soluciona el problema de su gestión, sino más bien todo lo contrario:

a) No están controlados por las directivas de la organización.

b) Suponen un aumento en costes en procesos de auditoría.

c) No es posible aplicar directivas de retención de mensajes.

d) Existe riesgo de pérdida de información.

e) Existe riesgo de fuga de información al no poder controlar el acceso al equipo físico.

f) Existe una alta dispersión de la información.

Es por ello que, para aquellas organizaciones que necesiten controlar, almacenar y auditar la información antigua, Exchange Server 2016 incorpora y mejora el archivo local (anteriormente denominado archivo personal), que ya se introdujo por primera vez en Exchange Server 2010.

Exchange Server 2016 permite aprovisionar el archivo de un usuario en la misma base de datos de buzones de correo que el buzón de correo principal del usuario, otra base de datos de buzones de correo en el mismo servidor de buzones, o bien una base de datos de buzones de correo en otro servidor de buzones en el mismo sitio de Directorio Activo.

Existen diversos métodos para mover mensajes a buzones de archivo:

a) **Mover o copiar mensajes manualmente.** Los usuarios de buzones de correo pueden mover o copiar de forma manual mensajes de su buzón de correo principal o de un archivo .pst a su buzón de archivo. El buzón de archivo aparece como otro buzón de correo o como un archivo .pst en Outlook y en Outlook en la Web.

b) **Mover o copiar mensajes mediante reglas de bandeja de entrada.** Los usuarios de buzones de correo pueden crear reglas de la bandeja de entrada en Outlook o en Outlook en la Web para mover automáticamente mensajes a una carpeta de su buzón de correo de archivo.

c) **Mover mensajes mediante directivas de retención.** Se pueden configurar directivas de retención para mover mensajes automáticamente al archivo. Además, los usuarios pueden aplicar una etiqueta personal para mover mensajes al archivo.

d) **Importar mensajes de archivos .pst.** En Exchange Server 2016, se puede usar una solicitud de importación de buzón de correo para importar mensajes de un archivo .pst al buzón de correo principal o al buzón de archivo de un usuario. Así mismo, Microsoft ha desarrollado la herramienta de captura PST para buscar los archivos .pst en los equipos de su organización e importar automáticamente los datos del archivo .pst a los archivos de los usuarios.

Nota: Puede descargar la herramienta de captura PST de Microsoft desde el siguiente enlace: https://docs.microsoft.com/es-es/office365/securitycompliance/find-copy-and-delete-pst-files-in-your-organization

Los mensajes se mueven a una carpeta en el buzón de archivo que tiene el mismo nombre que la carpeta de origen en el buzón de correo principal. Si no existe una carpeta con el mismo nombre en el buzón de archivo, se crea una cuando el asistente para carpetas administradas mueve un mensaje.

El hecho de recrear la misma jerarquía de carpetas en el buzón de archivo permite a los usuarios encontrar los mensajes con facilidad.

Durante la instalación de Exchange Server 2016, se crea una directiva de retención y de archivo predeterminada llamada "Directiva de MRM predeterminada". Esta directiva contiene etiquetas de retención con la acción mover a archivo, tal y como se muestra en la tabla siguiente:

Nombre de etiqueta de retención	Tipo de etiqueta	Descripción
Mover al archivo después de 2 años de forma predeterminada	Predeterminado (DPT)	Los mensajes se mueven automáticamente al buzón de archivo después de dos años. Se aplica a elementos de todo el buzón de correo que no tienen una etiqueta de retención aplicada explícitamente o heredada de la carpeta.
Mover al archivo después de 1 año en forma personal	Personal	Los mensajes se mueven automáticamente al buzón de archivo después de un año.
Mover al archivo después de 5 años en forma personal	Personal	Los mensajes se mueven automáticamente al buzón de correo de archivo después de cinco años.
Nunca mover al archivo en forma personal	Personal	Los mensajes nunca se mueven al buzón de correo de archivo.
Mover a archivo los elementos recuperables después de 14 días	Carpeta Elementos recuperables	Los mensajes se mueven de la carpeta Elementos recuperables del buzón de correo principal del usuario a la carpeta Elementos recuperables del buzón de archivo. Los usuarios que deseen intentar recuperar elementos eliminados en el archivo deben usar la característica de recuperar elementos eliminados en el buzón de archivo.

Si se habilita un archivo local para un usuario de buzón de correo y el buzón todavía no tiene asignada una directiva de retención, se le asignará automáticamente la directiva de retención y de archivo predeterminada.

Después de que el asistente para carpetas administradas procese el buzón de correo, estas etiquetas estarán a disposición del usuario, el cual puede etiquetar carpetas o mensajes para moverlos al buzón de archivo.

De forma predeterminada, los mensajes de correo electrónico de todo el buzón de correo se mueven una vez transcurridos dos años.

Antes de aprovisionar buzones de archivo para sus usuarios, se recomienda que les informe sobre las directivas de archivo que se aplicarán a sus buzones de correo, además de proporcionarles la formación y la documentación pertinentes para cubrir sus necesidades:

a) Funcionalidad disponible en el archivo, y las directivas de retención y de archivo predeterminadas.

b) Información sobre cuándo se pueden mover automáticamente mensajes al archivo.

c) Información sobre la jerarquía de carpetas creada en el buzón de archivo.

d) Cómo aplicar etiquetas personales (mostradas en el menú directiva de archivo en Outlook y en Outlook en la Web).

Los buzones de correo de archivo están diseñados para permitir a los usuarios almacenar el historial de datos de mensajería fuera de su buzón de correo principal.

Para eliminar la necesidad de tener archivos .pst, se recomienda proporcionar un buzón de archivo a los usuarios con límites de almacenamiento que cumplan con los requisitos del usuario.

No obstante, si se quiere conservar el control sobre las cuotas de almacenamiento y el crecimiento de los buzones de archivo para controlar los costos y la expansión, es posible configurar buzones de correo de archivo con una cuota de advertencia de archivo y una cuota de archivo.

Cuando un buzón de archivo supera la cuota de advertencia de archivo especificada, se registra un evento de advertencia en el registro de eventos de la aplicación. Cuando un buzón de archivo supera la cuota de archivo especificada, los mensajes ya no se mueven al archivo, se registra un evento de advertencia en el registro de eventos de la aplicación y se envía un mensaje de cuota al usuario del buzón de correo.

De forma predeterminada, en Exchange 2016, la cuota de advertencia de archivo está definida en 90 gigabytes (GB) y la cuota de archivo está definida en 100 GB.

Además, el uso de buzones de archivo local no supone una pérdida de funcionalidades de auditoría y control, ya que tanto la búsqueda de Exchange como la exhibición de documentos electrónicos pueden indizar elementos del archivo local.

a) **Exchange Search.** Para el servicio de búsqueda de Exchange, no hay ninguna diferencia entre el buzón de correo de archivo y el buzón de correo principal. El contenido de ambos buzones se indiza. Puesto que el buzón de archivo no se almacena en la caché del equipo de ningún usuario (aunque se use Outlook en el modo caché de Exchange), los resultados de búsqueda del archivo siempre se proporcionan mediante el servicio de búsqueda de Exchange. Si se realiza una búsqueda en todo el buzón de Outlook 2010 y superior y Outlook en la Web, los resultados de búsqueda incluyen el buzón de correo principal y el buzón de correo de archivo de los usuarios.

b) **Exhibición de documentos electrónicos local.** Cuando un administrador de descubrimiento realiza una búsqueda de exhibición de documentos electrónicos locales, también se busca en los buzones de archivo de los usuarios. No existe ninguna opción para excluir los buzones de archivo al crear una búsqueda de detección desde el Centro de Administración de Exchange (EAC). Si usa el Shell de administración de Exchange para crear una búsqueda de detección, se puede excluir el archivo con el modificador "DoNotIncludeArchive".

c) **Retención local y Retención para litigio.** Cuando se coloca un buzón de correo en retención local o suspensión por litigio, la retención se coloca tanto en el buzón de correo principal como en el buzón de correo de archivo.

d) **Carpeta Elementos recuperables.** El buzón de archivo contiene su propia carpeta de elementos recuperables y está sujeto a las mismas cuotas de carpeta de elementos recuperables que el buzón de correo principal.

e) **Archivar contenido de Skype Empresarial en Exchange.** Se pueden archivar conversaciones de mensajería instantánea y documentos de reuniones compartidos en línea en el buzón de correo principal del usuario. El buzón de correo debe estar ubicado en un servidor de buzón de correo de Exchange Server 2016 y debe tener implementado Microsoft Skype Empresarial 2015 en su organización.

7.9 PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)

Las directivas de prevención de pérdida de datos o DLP son paquetes que contienen conjuntos de condiciones, compuestos, a su vez, por reglas de transporte, acciones y excepciones que se activan para filtrar mensajes de correo y datos adjuntos.

Con las directivas de prevención de pérdida de datos, la organización puede realizar un control más exhaustivo sobre la información de carácter confidencial y el destino de ésta, evitando, por ejemplo, que un número de tarjeta de crédito termine en un destinatario fuera del control de la propia organización.

Nota: DLP es una característica premium que requiere una licencia de acceso de cliente (CAL) de Exchange Enterprise. Para obtener más información acerca de licencias de servidor y CAL, vea https://go.microsoft.com/fwlink/p/?linkid=237292.
En entornos híbridos donde se encuentran algunos buzones de correo en Exchange local y algunos están en Exchange Online, sólo se aplican las directivas de DLP en Exchange Online. Los mensajes que se envían entre usuarios locales no tienen directivas DLP aplicadas, debido a que los mensajes no se almacenan en el entorno local.

Exchange Server 2016 permite hacer uso de las directivas de pérdida de datos de tres formas diferentes:

a) Aplicar una plantilla de cuadro proporcionada en Exchange.

b) Importando directivas desarrolladas por empresas terceras fuera de la organización.

c) Creando una directiva personalizada sin ninguna condición preexistente.

Cuando se crean o se modifican directivas de DLP, se pueden incluir reglas que incorporen comprobaciones de información confidencial.

Las condiciones establecidas en una directiva, como la cantidad de veces que algo debe suceder antes de tomar una medida o exactamente el tipo de medida, se pueden personalizar en las directivas para que así satisfagan sus requisitos específicos de la organización.

Así mismo, para facilitar el uso de las reglas relacionadas con información confidencial, Microsoft proporciona de forma predeterminada plantillas de directivas que ya incluyen algunos de los tipos de información confidencial. Puede encontrar más información sobre las plantillas por defecto en el siguiente enlace:

https://docs.microsoft.com/es-es/exchange/security-and-compliance/data-loss-prevention/dlp-policy-templates

Sin embargo, no se pueden agregar condiciones para todos los tipos de información que figuran aquí en las plantillas de directivas, ya que las plantillas están diseñadas para ayudar a enfocarse en los tipos de datos relacionados con el cumplimiento más comunes dentro de su organización.

Se pueden crear varias directivas de DLP para su organización y habilitarlas todas para que se examinen diferentes tipos de información. También se puede crear una directiva de DLP que no esté basada en una plantilla existente.

Existe también la capacidad de creación de huellas digitales de documentos para crear fácilmente un tipo de información confidencial con base en un formulario estándar.

Exchange realiza fundamentalmente cinco pasos para comparar una regla prevención de pérdida de datos con los mensajes de correo electrónico.

En este ejemplo, donde se evalúa la aparición de patrones que pudieran coincidir con números de tarjetas de crédito, la regla se define de la siguiente forma.

```
<Entity id="50842eb7-edc8-4019-85dd-5a5c1f2bb085" patternsProximity="300" recommendedConfidence="85">
      <Pattern confidenceLevel="85">
        <IdMatch idRef="Func_credit_card" />
        <Any minMatches="1">
          <Match idRef="Keyword_cc_verification" />
          <Match idRef="Keyword_cc_name" />
          <Match idRef="Func_expiration_date" />
        </Any>
      </Pattern>
    </Entity>
```

Como se puede observar, la definición XML incluye la coincidencia de patrones, que mejora la probabilidad de que la regla detecte solo la información importante, y no información irrelevante relacionada.

En la regla de tarjetas de crédito, hay una sección de código XML para patrones, que incluye una coincidencia de identificadores principales y algunas pruebas adicionales:

a) <IdMatch idRef="Func_credit_card" />: requiere una coincidencia de una función, tarjeta de crédito con título, que se define internamente. Esta función incluye un par de validaciones de la forma siguiente:

b) Coincide con una expresión regular de 16 dígitos que también podría incluir variaciones como un delimitador de espacios para que también coincida con 4111 1111 1111 1111 o un delimitador de guiones para que también coincida con 4111-1111-1111-1111.

c) Evalúa el algoritmo de suma de comprobación Luhn, con el número de 16 dígitos para asegurar que la probabilidad de que se trate de un número de tarjeta de crédito sea alta.

d) Requiere una coincidencia obligatoria, tras la cual se evalúa la prueba adicional.

e) <Any minMatches="1">: esta sección indica que es necesaria la presencia de al menos uno de los siguientes elementos de prueba.

f) La prueba puede ser una coincidencia de uno de estos tres elementos:

i. <Match idRef="Keyword_cc_verification" />

ii. <Match idRef="Keyword_cc_name" />

iii. <Match idRef="Func_expiration_date" />

Esto significa que se requiere una lista de palabras clave de tarjetas de crédito, los nombres de las tarjetas de crédito o la fecha de caducidad. La fecha de caducidad se define y se evalúa internamente como otra función.

Por lo tanto, Exchange Server 2016 ejecuta los siguientes pasos para su evaluación:

Paso	Acción
1. Obtener contenido	Nombre Apellidos Visa: 4111 1111 1111 1111 Vence: 2/2018
2. Análisis de expresiones regulares	4111 1111 1111 1111 → se detectó un número de 16 dígitos
3. Análisis de funciones	4111 1111 1111 1111 → coincide con suma de comprobación 1234 1234 1234 1234 → no coincide
4. Pruebas adicionales	La palabra clave "Visa" está próxima al número. Una expresión regular para una fecha (2/2018) está próxima al número.
5. Veredicto	Hay una expresión regular que coincide con una suma de comprobación. Las pruebas adicionales aumentan la confianza.

Cada una de las directivas DLP que vienen preconfiguradas en Exchange Server 2016 o aquellas que se pudieran crear por parte de la organización pueden incluir definiciones de tipos de información confidencial.

Las definiciones de los tipos de información confidencial es la base sobre la cual se realiza la evaluación del contenido de los mensajes.

Un tipo de información confidencial se define con un patrón que se puede identificar mediante una expresión regular o una función. Además, las pruebas de corroboración (como las palabras clave y las sumas de comprobación) se pueden usar para identificar un tipo de información confidencial. La proximidad y el nivel de confianza también se emplean en el proceso de evaluación.

La prevención de pérdida de datos (DLP) de Exchange Server 2016 incluye 80 tipos de información confidencial listos para usarse en las directivas DLP. Puede encontrar más información sobre tipos de información sensible en el siguiente enlace:

https://docs.microsoft.com/es-es/exchange/policy-and-compliance/data-loss-prevention/sensitive-information-types?view=exchserver-2016

7.10 INFORMATION RIGHTS MANAGEMENT (IRM)

Los servicios de derechos de información constituyen otro pilar importante a la hora de proteger la información ante fuga de datos o accesos no autorizados a mensajes de correo electrónico o documentos adjuntos.

Los derechos de información no son una tecnología propia de Exchange, sino que más bien Exchange Server aprovecha esta tecnología para aplicar directivas de derechos de información a su propio contenido.

De igual forma, aplicaciones de cliente como Microsoft Outlook, Word, Excel o PowerPoint pueden hacer uso de las directivas de derechos de información que pudieran estar disponibles en la organización.

La tecnología IRM ayuda a proteger la información de la siguiente forma:

a) Impide que un destinatario autorizado para contenido protegido con IRM reenvíe, modifique, imprima, envíe por fax, guarde o corte y pegue el contenido.

b) Protege los formatos de archivo adjunto compatibles con el mismo nivel de protección que el del mensaje.

c) Admite la expiración de mensajes y datos adjuntos protegidos con IRM para que no se puedan visualizar después de un período específico.

d) Impide que se pueda copiar el contenido protegido con IRM por medio de la herramienta recortes de Windows.

Sin embargo, IRM no puede impedir que la información se copie mediante los métodos siguientes:

a) Programas de captura de pantalla de terceros.

b) Uso de dispositivos externos de imágenes como cámaras para fotografiar el contenido protegido con IRM que se muestra en la pantalla.

c) Usuarios que recuerdan o transcriben la información de forma manual.

El servicio Active Directory Rights Management Services (AD RMS) usa certificados y licencias basados en lenguaje de marcado con derechos extensible (XrML) para certificar equipos y usuarios, y para proteger el contenido.

Cuando se protegen contenidos con AD RMS, se adjunta una licencia XrML que contiene los derechos que los usuarios autorizados tienen con respecto al contenido.

A fin de obtener acceso al contenido protegido con IRM, las aplicaciones habilitadas para AD RMS deben obtener una licencia de uso para el usuario autorizado del clúster de AD RMS.

Se puede proteger el contenido con IRM desde múltiples puntos manuales o automáticos, incluyendo:

a) De forma manual por parte de los usuarios de Outlook. Los usuarios de Outlook pueden proteger los mensajes con IRM mediante las plantillas de directiva de derechos de AD RMS que tienen a su disposición. Este proceso usa la funcionalidad de IRM de Outlook, no de Exchange. Sin embargo, puede usar Exchange para obtener acceso a los mensajes y puede tomar acciones (como aplicar reglas de transporte) para cumplir con la directiva de mensajería de la organización.

b) De forma manual por parte de los usuarios de Outlook en la Web, cuando un administrador habilita IRM en Outlook en el web (anteriormente conocido como Outlook Web App), los usuarios pueden proteger con IRM los mensajes que van a enviarán y ver los mensajes protegidos por IRM que reciben.

c) Manualmente por parte de los usuarios de ActiveSync, cuando un administrador habilita IRM Exchange ActiveSync los usuarios pueden ver, responder, reenviar y crear mensajes protegidos por IRM en dispositivos ActiveSync.

d) De forma automática en Outlook. Se pueden crear reglas de protección de Outlook para aplicar la protección de IRM automática a los mensajes en Outlook. Las reglas de protección de Outlook se implementan de forma automática en los clientes y aplica la protección de IRM cuando el usuario redacta un mensaje.

e) De forma automática en los servidores de buzones de correo. los administradores pueden crear reglas de flujo de correo (también conocida como reglas de transporte) automáticamente proteger con IRM los mensajes que coinciden con las condiciones especificadas.

Es necesario que se pueda obtener acceso al contenido cifrado del mensaje a fin de exigir el cumplimiento de directivas de mensajería y para el cumplimiento de las reglamentaciones.

A fin de cumplir con los requisitos de detección debido a litigios, auditorías reglamentarias o investigaciones internas, es necesario que se pueda buscar mensajes cifrados.

Para ayudar con estas tareas, Exchange 2016 incluye las siguientes características de IRM:

a) **Descifrado de transporte.** Permite el acceso al contenido del mensaje por los agentes de transporte que están instalados en los servidores de Exchange.

b) **Descifrado de informe de diario.** Permite al registro en diario (Standard o Premium) guardar una copia de texto sin cifrar de los mensajes protegidos con IRM en informes de diario.

c) **Descifrado IRM para Exchange Search.** El servicio de búsqueda de Exchange puede indexar el contenido de mensajes protegidos con IRM con el descifrado IRM para Exchange Search. Cuando un administrador de detección realiza una búsqueda de exhibición de documentos electrónicos en contexto, los mensajes protegidos con IRM que se indexaron se devuelven en los resultados de la búsqueda.

Para habilitar todas estas características de descifrado, los servidores de Exchange deben tener acceso al mensaje. Esto se logra al agregar el buzón de correo de federación, un buzón del sistema creado por el programa de instalación de Exchange, al grupo de superusuarios del servidor de AD RMS.

En Exchange 2016, la función de IRM se habilita mediante los agentes de transporte en el servicio de transporte de los servidores de buzones de correo. El programa de instalación de Exchange instala los agentes de IRM en un servidor de buzones de correo.

Nota: No se puede controlar a los agentes IRM mediante las tareas de administración para los agentes de transporte. Los agentes de IRM son agentes integrados y por lo tanto no están incluidos en la lista de agentes que devuelve el cmdlet "Get-TransportAgent".

En la siguiente tabla se enumeran los agentes de IRM implementados en el servicio de transporte en servidores de buzones de correo.

Agente	Evento	Función
Agente de descifrado de informes de diario.	OnCategorizedMessage	Proporciona una copia de texto sin cifrar de los mensajes protegidos por IRM que se adjuntan a los informes de diario.
Agente de licencias previas.	OnRoutedMessage	Adjunta una licencia previa a los mensajes protegidos con IRM.
Agente de descifrado de RMS.	OnSubmittedMessage	Descifra los mensajes para permitir el acceso a los agentes de transporte.

Agente	Evento	Función
Agente de cifrado de RMS.	OnRoutedMessage	Aplica la protección IRM a los mensajes que marcó el agente de reglas de transporte y vuelve a cifrar los mensajes descifrados de transporte.
Agente de descifrado de protocolo RMS	OnEndOfData	Descifra los mensajes protegidos con IRM para permitir el acceso al contenido de mensaje por los agentes de transporte.
Agente de reglas de transporte.	OnRoutedMessage	Marca los mensajes que coinciden con las condiciones en una regla de protección de transporte para estar protegido por IRM por el agente de cifrado de RMS.

7.10.1 PROTECCIÓN AUTOMÁTICA MEDIANTE REGLAS DE TRANSPORTE

Los mensajes que contienen información crítica para la empresa se pueden identificar mediante una combinación de condiciones de reglas de transporte, incluidas expresiones regulares que identifican patrones de texto tales como números de seguridad social.

Las organizaciones requieren diferentes niveles de protección de la información confidencial. Es por ello que algunos tipos de información pueden restringirse a empleados, contratistas o asociados; mientras que otros tipos pueden restringirse solamente a empleados a tiempo completo.

El nivel deseado de protección se puede aplicar a los mensajes mediante la aplicación de una plantilla de directivas de derechos adecuada.

Por ejemplo, los usuarios pueden marcar los mensajes o datos adjuntos de correo electrónico como "Información confidencial de la empresa", pudiendo posteriormente crear una regla de protección de transporte para inspeccionar el contenido de mensajes en busca de las palabras "Información confidencial de la empresa" y proteger el mensaje con IRM de manera automática.

Así mismo, la protección persistente no solo se aplica al mensaje como tal, sino también a los diferentes tipos de adjuntos de correo electrónico.

Es habitual que los usuarios envíen información crítica para la empresa en documentos adjuntos de correo electrónico como Microsoft Office Word, Excel y PowerPoint.

Todos estos formatos de archivos admiten la protección persistente a través de IRM y, de esta forma, se puede garantizar que la información crítica para la empresa contenida en estos documentos está protegida adecuadamente.

Las reglas de protección de transporte aplican la misma protección a los mensajes y los datos adjuntos de correo electrónico en formatos de archivos admitidos.

Cuando se utilizan reglas de protección de transporte para mensajes protegidos con IRM en función de condiciones de reglas, el agente de reglas de transporte en el servidor de buzones inspecciona los mensajes.

Si el mensaje cumple con todas las condiciones y ninguna de las excepciones, lo etiqueta para ser protegido con IRM. Posteriormente, el agente de cifrado, un agente de transporte integrado que se activa con el evento "OnRoutedMessage", aplica realmente la protección IRM al mensaje.

El agente de cifrado actúa en mensajes solo si IRM está habilitado para mensajes internos.

Cuando se reinicia el servicio de transporte y se procesa el primer mensaje que requiere el cifrado de IRM, el agente de cifrado debe ser capaz de conectarse con un servidor de AD RMS de la organización. Para los mensajes posteriores, el agente no necesita establecer contacto con el servidor de AD RMS.

Si se produce un error en el cifrado de un mensaje debido a condiciones transitorias, Exchange vuelve a intentar cifrar el mensaje tres veces en intervalos de 10 minutos. Después de los tres intentos, si no se puede cifrar el mensaje, éste no se entrega a los destinatarios y se envía un mensaje de no entrega NDR al remitente.

Cuando se planifique el uso de reglas de protección de transporte, se debe considerar el tipo de información que se desea proteger y planificar la creación de reglas de manera consecuente.

En Exchange 2016, las reglas de transporte tienen una gran cantidad de predicados que permiten inspeccionar el contenido de los mensajes, incluidos los datos adjuntos admitidos, los encabezados de mensaje, las direcciones del remitente y del destinatario, los atributos de Directorio Activo tales como departamento, pertenencia a grupos de distribución y relaciones de administración del remitente con los destinatarios.

Del mismo modo, se debe tener en cuenta el tráfico de mensajería de la organización y la cantidad de mensajes que se protegerán mediante las reglas de protección de transporte ya que la aplicación de la protección de IRM a una gran cantidad de mensajes requiere más recursos en el servidor buzones. Además, la protección de una gran cantidad de mensajes o de todos los mensajes también afecta la experiencia del cliente, en especial, para los usuarios de Microsoft Outlook.

7.10.2PROTECCIÓN AUTOMÁTICA DE IRM EN OUTLOOK

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.

Al crear reglas de protección de Outlook en un servidor de Exchange Server 2016, las reglas se distribuyen automáticamente a Outlook por medio de los servicios Web Exchange.

Para que Outlook aplique la regla, la plantilla de directivas de derechos de AD RMS especificada debe estar disponible en los equipos de los usuarios.

Las reglas de protección de Outlook son similares a las reglas de protección de transporte. Ambos tipos se aplican según las condiciones de los mensajes y ambos protegen los mensajes mediante la aplicación de una plantilla de protección de derechos de AD RMS. Sin embargo, las reglas de protección de transporte se aplican en el servicio de transporte en el servidor de buzones por parte del agente de reglas de transporte, mientras que las reglas de protección de Outlook se aplican en el cliente Outlook, antes de que el mensaje salga del equipo del usuario.

Nota: Los mensajes protegidos por una regla de protección de Outlook entran en la canalización de transporte con la protección de IRM ya aplicada. Así mismo, los mensajes protegidos con una regla de protección de Outlook también quedan almacenados en formato cifrado en la carpeta de elementos enviados del buzón de correo del remitente.

Para crear reglas de protección de Outlook, es necesario utilizar el cmdlet "New-OutlookProtectionRule" en el Shell de administración de Exchange.

Al crear una regla se puede especificar si el usuario podrá invalidarla, ya sea eliminando la protección de IRM o aplicando otra plantilla de directivas de derechos de AD RMS a la especificada en la regla.

Si un usuario invalida la protección de IRM aplicada por una regla de protección de Outlook, Outlook inserta el encabezado "X-MS-Outlook-Client-Rule-Overridden" en el mensaje original, lo cual permite determinar que el usuario ha invalidado la regla.

7.11 S/MIME

La primera versión de S/MIME (Secure / Multipurpose Internet Mail Extensions) fue desarrollada en 1995 por una serie de proveedores de seguridad, entre ellos RSA. Fue una de las distintas especificaciones para la seguridad de los mensajes. Pretty Good Privacy (PGP) es un ejemplo de otra especificación diferente para la seguridad de los mensajes.

Cuando se publicó la versión 1 de S/MIME, no existía ningún estándar único reconocido para la seguridad de los mensajes, sino que existían varios estándares en competencia. En 1998, la situación empezó a cambiar con la aparición de la versión 2 de S/MIME, la cual, a diferencia de la versión 1, la versión 2 de S/MIME fue sometida al Internet Engineering Task Force (IETF, Grupo de trabajo de ingeniería en Internet) para su consideración como estándar de Internet.

Con este paso, S/MIME pasó de ser un posible estándar entre otros muchos a ser el principal contendiente para un estándar de seguridad de los mensajes. La versión 2 de S/MIME consta de dos Request for Comments (RFC, Solicitud de comentarios) de IETF: RFC 2311 (http://www.ietf.org/rfc/rfc2311.txt), que establecía el estándar para los mensajes y RFC 2312 (http://www.ietf.org/rfc/rfc2312.txt), que establecía el estándar para el tratamiento de certificados.

Juntas, estas dos RFC proporcionaron el primer marco de trabajo basado en estándares de Internet que los proveedores podían seguir para ofrecer soluciones interoperables de seguridad de los mensajes. Con la versión 2 de S/MIME, S/MIME se convierte en el estándar para la seguridad de los mensajes.

En 1999, el IETF propuso la versión 3 de S/MIME para mejorar la capacidad de S/MIME. La RFC 2632 (http://www.ietf.org/rfc/rfc2632.txt) se basó en el trabajo realizado en la RFC 2311 para especificar los estándares para los mensajes S/MIME y la RFC 2633 (http://www.ietf.org/rfc/rfc2633.txt) mejoró la especificación del tratamiento de certificados contenida en la RFC 2312.

La RFC 2634 (http://www.ietf.org/rfc/rfc2634.txt) amplió las capacidades generales al agregar otros servicios adicionales a S/MIME, como confirmaciones seguras, triple envoltorio y etiquetas de seguridad.

La versión 3 de S/MIME ha logrado una amplia aceptación como estándar para la seguridad de los mensajes en muchas organizaciones.

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.

También permite garantizar que el mensaje proviene del remitente específico y no de alguien que pretende ser el remitente.

Para ello, S/MIME proporciona servicios de seguridad criptográfica como autenticación, integridad de mensajes y no rechazo de origen (usando firmas digitales). También ayuda a mejorar la privacidad y la seguridad de los datos (mediante cifrado) en la mensajería electrónica.

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 siguientes 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.

Sin embargo, las firmas digitales por si solas, no ofrecer confidencialidad de la información o los datos contenidos en el mensaje. Es por ello que S/MIME también ofrece capacidad de cifrado del contenido para preservar la confidencialidad del mensaje cuando se envía a través de canales de comunicaciones públicos o no confiables.

El cifrado de mensajes ofrece una solución para la revelación de información. De forma predeterminada, el protocolo SMTP no protege los mensajes ya que su contenido es texto plano y puede ser leído por cualquiera que lo vea mientras viaja o que lo vea donde está almacenado.

S/MIME resuelve estos problemas mediante el uso del cifrado, ofreciendo, además, 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. El cifrado ofrece confidencialidad mientras el mensaje está en tránsito y también mientras está almacenado.

b) **Integridad de los datos.** Como ocurre con las firmas digitales, el cifrado de mensajes ofrece servicios de integridad de los datos como resultado de las operaciones específicas que hacen posible el cifrado.

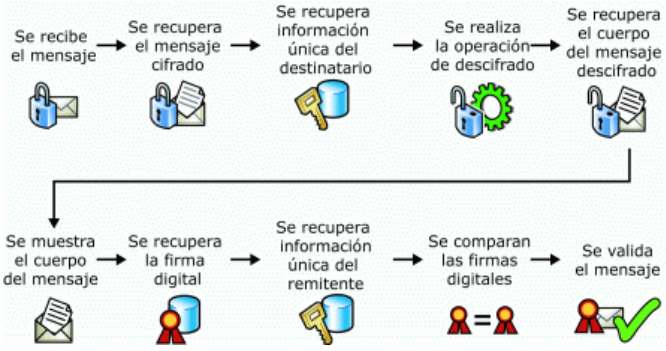
Las firmas digitales y el cifrado de mensajes no son servicios mutuamente exclusivos. Cada servicio resuelve determinados problemas de seguridad.

Las firmas digitales resuelven los problemas de autenticación y no rechazo, mientras que el cifrado de mensajes resuelve los problemas de confidencialidad. Como cada uno de estos servicios resuelve problemas diferentes, una estrategia de seguridad adecuada de los mensajes suele requerir ambos servicios al mismo tiempo.

A continuación, se muestra la secuencia de firma y cifrado de un mensaje de correo electrónico.

a) Firma y cifrado durante el envío del mensaje.

b) Validación de la firma y descifrado del mensaje en la recepción de éste.



Así mismo, una de las mejoras de S/MIME versión 3 que merece la pena destacar es el "triple envoltorio". Un mensaje S/MIME con triple envoltorio es aquel que se firma, se cifra y se firma de nuevo.

Este nivel adicional de cifrado proporciona un nivel adicional de seguridad. Cuando los usuarios firman y cifran mensajes con Outlook Web Access con el control S/MIME, el mensaje tiene triple envoltorio automáticamente. Los clientes Outlook no aplican triple envoltorio a los mensajes, pero pueden leer este tipo de mensajes.

Un administrador de Exchange puede habilitar la seguridad basada en S/MIME en Outlook en la Web, o en clientes de correo electrónico como Outlook y dispositivos móviles compatibles.

Para usar S/MIME en las versiones admitidas de Outlook o ActiveSync, los usuarios deben disponer de al menos un certificado emitidos con fines de firma y cifrado, y los datos publicados en el servicio de dominio de Directorio Activo.

Los pasos que debe seguir para configurar S/MIME con cada uno de los clientes admitidos es ligeramente diferente según cuál elija, sin embargo, por lo general, deberá realizar lo siguiente:

a) Implementar una entidad emisora de certificados basada en Windows y configurar una infraestructura de clave pública para emitir certificados S/MIME.

b) Publicar el certificado de usuario en una cuenta local de Directorio Activo en los atributos "UserSMIMECertificate" y "UserCertificate".

c) Crear una colección virtual de certificados para validar S/MIME. OWA usa esta información para validar la firma de un correo electrónico y garantizar que se ha firmado con un certificado de confianza.

d) Configurar el extremo de Outlook o EAS para usar S/MIME.

7.12 REGISTRO DE AUDITORÍA DE ADMINISTRADOR

El registro de auditoría de administrador es una característica que permite auditar las operaciones realizadas en los servidores Exchange de la organización y que pueden afectar a usuarios, servidores o a la propia seguridad de la organización.

De forma predeterminada, el registro de auditoría de administrador está habilitado en las nuevas instalaciones de Exchange Server.

Se auditan los cmdlets que se ejecutan directamente en el Shell de administración de Exchange. Además, también se registran las operaciones realizadas con el Centro de administración de Exchange (EAC), ya que ejecutan cmdlets en segundo plano.

Los cmdlets, independientemente de donde se ejecuten, se auditan si un cmdlet está en la lista de auditoría del cmdlet y si uno o más parámetros de ese cmdlet están en la lista de auditoría del parámetro. Los cmdlets "Get-" y "Search-" no se registran.

La finalidad del registro de auditoría es mostrar qué acciones se han realizado para modificar objetos en una organización de Exchange.

Nota: Un comando puede tardar hasta 15 minutos a partir de su ejecución en aparecer en los resultados de búsqueda del registro de auditoría. Esto se debe a que las entradas del registro de auditoría deben indizarse antes de que puedan realizarse búsquedas en ellas. Si un comando no aparece en el registro de auditoría del administrador, espere unos minutos y vuelva a hacer la búsqueda. Los cambios realizados en la configuración del registro de auditoría del administrador siempre se registran, independientemente de si el cdmlet "Set-AdministratorAuditLog" está incluido en la lista de cmdlets que se auditan y de si el registro de auditoría está habilitado o deshabilitado.

Cuando se ejecuta un comando, Exchange inspecciona el cmdlet que se ha utilizado. Si el cmdlet que se ejecutó coincide con alguno de los cmdlets proporcionados con el parámetro "AdminAuditLogConfigCmdlets", Exchange comprueba luego los parámetros especificados en el parámetro "AdminAuditLogConfigParameters".

Si uno o más parámetros de la lista de parámetros coinciden, Exchange registra el cmdlet que se ejecutó en el buzón de correo especificado usando el parámetro "AdminAuditLogMailbox".

De forma predeterminada, el registro de auditoría está configurado para almacenar entradas de registro de auditoría durante 90 días. Después de 90 días, se elimina la entrada del registro de auditoría.

Se puede modificar el límite de antigüedad del registro de auditoría mediante el parámetro "AdminAuditLogAgeLimit".

De manera predeterminada, el registro de auditoría de administrador registra solo el nombre del cmdlet, sus parámetros (y los valores especificados), el objeto que se modificó y quién, cuándo y en qué servidor se ejecutó el cmdlet.

El registro de auditoría de administrador no registra qué propiedades se modificaron en el objeto, sin embargo, si fuese necesario para cumplir con normativas internas de la organización, se puede habilitar el registro detallado configurando el parámetro "LogLevel" en Verbose.

Cuando habilita el registro detallado, además de la información registrada de manera predeterminada, se incluyen en el registro de auditoría las propiedades modificadas en un objeto, incluidos sus valores antiguos y nuevos.

Los registros de auditoría se almacenan en un buzón de correo oculto de arbitraje dedicado, al que solamente se puede obtener acceso mediante el EAC o los cmdlets "Search-AdminAuditLog" o "New-AdminAuditLogSearch". No se puede abrir mediante Microsoft Outlook en la Web o Microsoft Outlook.

A continuación, se muestran los campos de entrada del registro de auditoría.

Campo	Descripción
RunspaceId	Exchange utiliza este campo de manera interna.
ObjectModified	Este campo contiene el objeto modificado por el cmdlet especificado en el campo CmdletName.
CmdletName	Este campo contiene en nombre del cmdlet ejecutado por el usuario en el campo Caller.
CmdletParameters	Este campo contiene los parámetros especificados cuando se ejecutó el cmdlet en el campo CmdletName. Además, se almacena el valor especificado con el parámetro (si corresponde), aunque no es visible en los resultados predeterminados.
ModifiedProperties	Este campo contiene las propiedades modificadas en el objeto en el campo ObjectModified. Además, en este campo se almacenan el valor anterior de la propiedad y el nuevo valor almacenado, aunque no están visibles en los resultados predeterminados.
Caller	Este campo contiene la cuenta de usuario del usuario que ejecutó el cmdlet en el campo CmdletName.
Succeeded	Este campo especifica si el cmdlet del campo CmdletName se ejecutó correctamente. El valor es True o False.

Campo	Descripción
Error	Este campo contiene el mensaje de error generado si el cmdlet del campo CmdletName no se pudo completar correctamente.
RunDate	Este campo contiene la fecha y la hora en las que se ejecutó el cmdlet en el campo CmdletName. La fecha y la hora se almacenan en formato de hora universal coordinada (UTC).
OriginatingServer	Este campo indica el servidor en el cual se ejecutó el cmdlet especificado en el campo CmdletName.
Identity	Exchange utiliza este campo de manera interna.
IsValid	Exchange utiliza este campo de manera interna.
ObjectState	Exchange utiliza este campo de manera interna.

La página de auditoría del EAC tiene diversos informes que proporcionan información sobre varios tipos de cambios de configuración administrativa y de cumplimiento. Los informes siguientes proporcionan información acerca de los cambios de configuración en la organización:

a) **Informe de grupo de roles de administrador.** Este informe permite buscar cambios de grupos de roles de administración dentro de un período especificado. Los resultados que se devuelven muestran los grupos de funciones que han sido modificados, quien los modificó y cuándo, y qué cambios se realizaron. Se puede devolver un máximo de 3.000 entradas. Si es posible que la búsqueda devuelva más de 3.000 entradas, se recomienda utilizar el informe de **registro de auditoría de administrador** o el cmdlet **"Search-AdminAuditLog"**.

b) **Registro de auditoría de administrador.** Este informe permite exportar a un archivo XML las entradas del registro de auditoría registradas en un período de tiempo especificado y, a continuación, enviar el archivo por correo electrónico al destinatario que se especifique.

De igual forma, cuando ejecuta el cmdlet "Search-AdminAuditLog", se devuelven todas las entradas del registro de auditoría que coinciden con el criterio de búsqueda especificado. Se pueden especificar los siguientes criterios de búsqueda:

a) **Cmdlets.** Especifica los cmdlets que se desea buscar en el registro de auditoría de administrador.

b) **Parámetros.** Especifica los parámetros, separados por comas, que se desea buscar en el registro de auditoría de administrador. Solo se pueden buscar parámetros si se especifica un cmdlet para buscar.

c) **Fecha de finalización.** Reduce el ámbito de los resultados del registro de auditoría de administrador a las entradas de registro correspondientes a la fecha especificada o a las fechas anteriores a esta.

d) **Fecha de inicio.** Reduce el ámbito de los resultados del registro de auditoría de administrador a las entradas de registro correspondientes a la fecha especificada o a las fechas posteriores a esta.

e) **Id. de objeto.** Especifica que solamente se devuelvan las entradas del registro de auditoría de administrador que contengan los objetos modificados especificados

f) **Id. de usuario.** Especifica que solamente se devuelvan las entradas del registro de auditoría de administrador que contengan el identificador especificado del usuario que ejecutó el cmdlet.

g) **Finalización satisfactoria.** Especifica si solamente se deben devolver las entradas de registro de auditoría de administrador que indicaron acierto o error.

De forma predeterminada, solamente se devuelven las primeras 1.000 entradas del registro que coinciden con los criterios especificados. Sin embargo, se puede invalidar esta configuración predeterminada y habilitar la devolución de una mayor o menor cantidad de entradas con el parámetro "ResultSize".

Por otro lado, el cmdlet "New-AdminAuditLogSearch" busca el registro de auditoría al igual que el cmdlet "Search-AdminAuditLog". Sin embargo, en lugar de mostrar los resultados de la búsqueda del registro de auditoría en el Shell, el cmdlet "New-AdminAuditLogSearch" realiza la búsqueda y, a continuación, envía los resultados de la búsqueda por correo electrónico al destinatario que usted especifica.

Los resultados se incluyen como datos adjuntos XML en el mensaje de correo electrónico.

Se pueden utilizar los mismos criterios de búsqueda con el cmdlet "New-AdminAuditLogSearch" que con el cdmlet "Search-AdminAuditLog".

Después de ejecutar el cmdlet "New-AdminAuditLogSearch", Exchange puede tardar hasta 15 minutos para entregar el informe al destinatario especificado. Así mismo, el informe adjunto en un archivo XML puede tener un máximo de 10 megabytes (MB).

El registro de auditoría de administrador usa la replicación de Directorio Activo para replicar las opciones de configuración que se especifiquen en los controladores de dominio de la organización.

En función de las opciones de replicación, es posible que los cambios que se realicen no se apliquen de inmediato a todos los servidores que ejecutan Exchange Server 2016 en la organización.