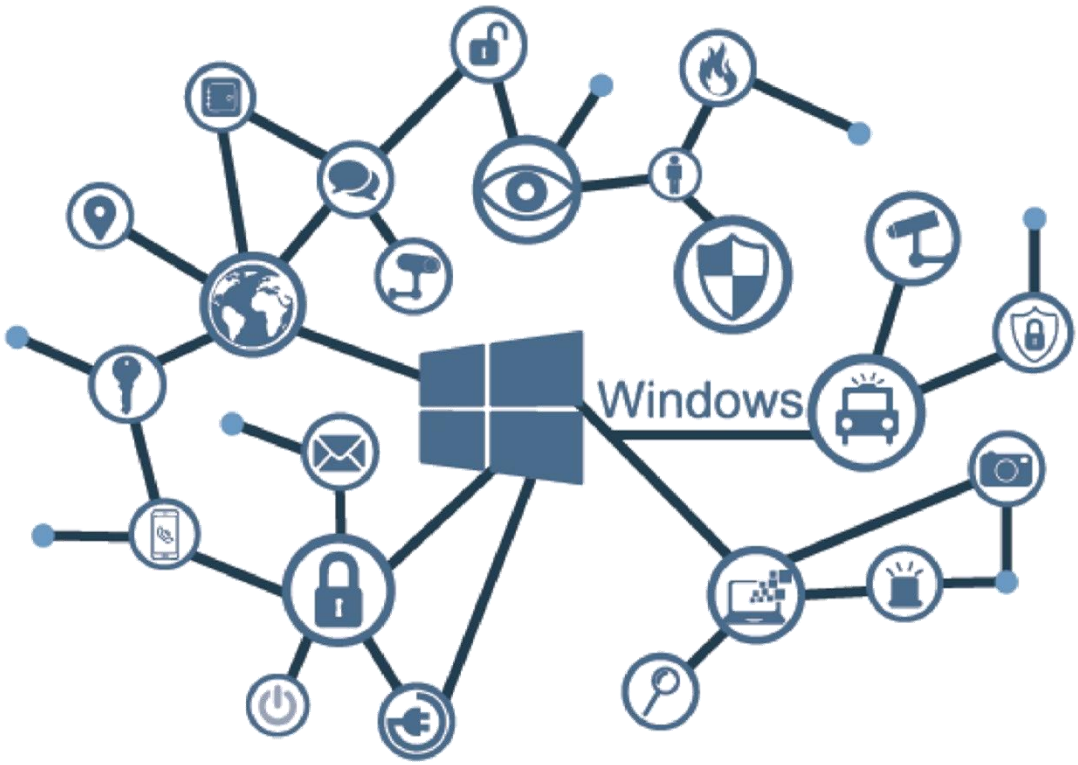
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 576A25

APLICACIÓN DE SEGURIDAD SOBRE MICROSOFT EXCHANGE SUBSCRIPTION EDITION



ENERO 2026

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

Firmado digitalmente por CCN
Nombre de reconocimiento (DN): c=ES, l=MADRID, o=CCN, ou=SELLO ELECTRONICO, 2.5.4.97=VATES-S2800155J, serialNumber=S2800155J, cn=CCN
Fecha: 2026.09.09 14:17:41 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO 083-26-274-1 (edición en línea)

Fecha de Edición: enero de 2026

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

INDICE

1. INTRODUCCIÓN 4

2. OBJETO 4

3. ALCANCE 6

4. DESCRIPCIÓN DE USO DE ESTA GUÍA 7

4.1. Requisitos Previos para Microsoft Exchange Server Subscription Edition 7

4.2. Instalación y Aplicación de Seguridad sobre Rol IIS 7

5. PERFILADO DE CUMPLIMIENTO TÉCNICO 8

ANEXO A. Aplicación de Seguridad sobre Microsoft Exchange SE 10

ANEXO A.1. Implementación de Políticas de Seguridad sobre el Dominio 11

ANEXO A.2. Configuraciones Adicionales 31

ANEXO A.2.1. Configuración de Certificados 31

ANEXO A.2.2. Asignación de Permisos y Roles 46

ANEXO A.2.3. Configuración de Registro de Actividad 53

ANEXO A.2.4. Configuración de Registro de Seguimiento de Mensajes 57

ANEXO A.2.5. Configuración de Registro de la Gestión de Incidentes 60

ANEXO A.3. Comprobaciones 64

1. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el **Centro Criptológico Nacional (en adelante, CCN)** 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** (en adelante, ENS) y, de igual modo, de obligado cumplimiento para los sistemas que manejen **Información Clasificada** de ámbito NACIONAL tal y como se expone en el "Artículo 2" del propio ENS. Esto último sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa de aplicación. De igual modo se aplica a los sistemas de información de las entidades del sector privado cuando, según el ENS, "de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público".

La **serie CCN-STIC-500** se ha diseñado de manera incremental. Así, dependiendo del sistema operativo, los productos que implemente y los servicios que ofrezca, se aplicarán consecutivamente varias de estas guías para asegurar en su totalidad todos los elementos del sistema de información. En este sentido, se deberán aplicar las guías correspondientes dependiendo del entorno que se esté asegurando.

Por ejemplo, en el caso de un entorno para un servidor miembro de dominio con Microsoft Windows Server 2025, en el que se instale Microsoft Exchange Subscription Edition, deberán aplicarse las guías técnicas más recientes publicadas en el portal web del CCN-CERT:

a) Guía CCN-STIC-570A25 en el servidor miembro con Windows Server 2025.

b) Guía CCN-STIC-574A25 sobre Internet Information Services (IIS), para la configuración segura del servicio

c) Guía CCN-STIC-576A25 sobre Microsoft Exchange, aplicable a los servidores que alojarán el servicio de Exchange.

Nota: actualmente, las guías Microsoft publicadas en la serie **800** están orientadas a servicios en la nube adaptados al ENS. Para el despliegue en infraestructura propia, las guías aplicables se encuentran en la serie **500**, que recoge la documentación más actualizada para estos escenarios.

2. OBJETO

El propósito de esta guía de seguridad es proporcionar los elementos y directrices para aplicar y garantizar la seguridad en equipos que implementen el aplicativo **Microsoft Exchange Subscription Edition** en un entorno de dominio.

La configuración que se aplica a través de la presente guía establece las restricciones necesarias para minimizar la superficie de ataque y posibles riesgos asociados a la implementación de este servicio. En algunos casos, y dependiendo de la funcionalidad asociada al servidor, podría ser necesario modificar la configuración planteada en la presente guía.

Así, se entenderá que la implementación del servicio Microsoft Exchange Subscription Edition, dependerá de las necesidades peculiares y servicios prestados por la entidad que lo aplica. Consecuentemente, aquellas plantillas y guías de seguridad generadas recogerán aquellas pautas generales de seguridad que permitan el cumplimiento de los requisitos y estándares mínimos de seguridad establecidos en el ENS, así como aquellas condiciones que, según la normativa nacional de aplicación, se requieran para el manejo de Información Clasificada.

La definición de las medidas de seguridad asociadas a la presente guía se basan, principalmente, en las necesidades técnicas recogidas en el "Anexo II: Medidas de Seguridad", así como aquellas disposiciones establecidas por el CCN en la Instrucción Técnica de Seguridad de las TIC (CCN-STIC-301) y otras normativas nacionales de aplicación, que permitan una aproximación al Marco Moderno de Seguridad.

Este marco de aplicación basa sus pilares fundamentales en los siguientes objetivos:

- Las medidas a adoptar estarán condicionadas no solo por la normativa aplicable y el presente documento, sino también por el análisis de riesgos preceptivo de cada escenario (Sistema de Información Clasificada, en adelante, CIS), la probabilidad de materialización de la amenaza y la superficie de exposición del sistema.
- Será adaptable en la aplicación de medidas, evitando una aplicación monolítica y estanca utilizando la Declaración de Aplicabilidad Técnica o Perfil de Cumplimiento Técnico Específico (en adelante, PCTE) como elemento fundamental sobre el que vertebrar la seguridad. Se tomará de igual modo en cuenta el Perfil de Cumplimiento Específico (en adelante, PCE) aplicable al conjunto del organismo y sus sistemas de información.
- El PCTE y las medidas establecidas por medio del presente documento cumplen los requisitos técnicos para que los sistemas TIC se adapten a cualquier CLASIFICACIÓN DE LA INFORMACIÓN tomando en consideración la categorización de los sistemas definida en el ENS.
- Las guías se revisarán y se actualizarán según las nuevas amenazas, avances tecnológicos y estado de arte tecnológico en ciberseguridad, así como nuevas configuraciones de seguridad proporcionadas por los productos.

La configuración planteada se ha diseñado para adaptarse a las características específicas de cada entorno, en función de las necesidades de este, pero garantizando el cumplimiento de los requisitos mínimos de seguridad definidos bajo el PCTE. En caso de no poder aplicar los requisitos mencionados, estos deberán ser compensados por medio de medidas técnicas complementarias (vigilancia) y/o compensatorias.

Para la elaboración de esta guía, se ha realizado una revisión exhaustiva de las distintas configuraciones de seguridad disponibles en los sistemas operativos Windows Server, alineándolas y clasificándolas en función de los requisitos definidos por las normativas aplicables.

De esta forma, se pretende dar mayor coherencia al conjunto de medidas resultantes, siendo necesario implementar únicamente aquellas que realmente son de aplicación según el tipo de sistema de información y datos que maneja.

3. ALCANCE

La presente guía se ha elaborado para proporcionar información específica para realizar una implementación de la solución de Microsoft Exchange Server Subscription Edition en una configuración restrictiva de seguridad. Se incluyen, además, operaciones básicas de administración.

El escenario en el cual está basada la guía CCN-STIC-576A25 tiene las siguientes características técnicas:

a) Un único bosque de Directorio Activo (en adelante, AD).

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 2025.

e) Dos servidores miembros del dominio basado en Windows Server 2025.

f) Una Autoridad de Certificación (en adelante, CA) basada en Windows Server 2025.

g) En los servidores miembro, se instalan los siguientes roles:

   a. Servidor de buzones.

   b. Base de datos.

Este documento incluye:

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

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

c) Descripción de la seguridad en Microsoft Exchange Server Subscription Edition. Completa descripción de los mecanismos de seguridad, autenticación y autorización utilizados en Microsoft Exchange Server Subscription Edition.

d) Guía paso a paso. Permite implementar y establecer las configuraciones de seguridad necesarias en una arquitectura de un servidor con Microsoft Exchange Server Subscription Edition.

Nota: No se contemplan procedimientos de migración desde versiones anteriores de Microsoft Exchange.

4. DESCRIPCIÓN DE USO DE ESTA GUÍA

Para comprender la presente guía de seguridad, es fundamental explicar el proceso que describe y los recursos que se ponen a disposición para garantizar una implementación segura y conforme a las buenas prácticas. Este proceso se compone de las fases que se describen a continuación.

4.1. Requisitos Previos para Microsoft Exchange Server Subscription Edition

Antes de aplicar las medidas de seguridad indicadas en esta guía, se deben considerar los siguientes aspectos:

- **Cumplimiento de requisitos de instalación:** Además de los requisitos generales para la instalación de Microsoft Exchange Server Subscription Edition, será necesario verificar:
    - Compatibilidad del sistema operativo (Windows Server en la versión soportada por Microsoft Exchange Subscription Edition).
    - Configuración de hardware mínima: unidad central de almacenamiento (en adelante, CPU), memoria y almacenamiento).
    - Versiones y parches actualizados del sistema operativo, seguridad y componentes críticos.
- **Requisitos técnicos específicos:** Se deben cumplir los requisitos definidos por Microsoft Exchange, incluyendo:
    - Servicios independientes: Internet Information Services (IIS) 10, .NET Framework, Windows Management Framework, entre otros.
    - Configuración de red: Domain Name System (en adelante, DNS), conectividad, certificados válidos.
    - Políticas de seguridad: aplicación de directivas de grupo (en adelante, GPO) base de Microsoft Windows Server de la guía STIC más moderna aplicable.
- **Comprobación de otros servicios y aplicaciones:** si se van a integrar aplicaciones adicionales (por ejemplo, antivirus, soluciones antimalware, herramientas de monitorización), se debe garantizar su compatibilidad y que no interfieran con la configuración segura de Exchange.

4.2. Instalación y Aplicación de Seguridad sobre Rol IIS

Antes de proceder con la instalación de Microsoft Exchange Server, es imprescindible aplicar medidas de seguridad sobre el sistema operativo y el rol Internet Information Services (IIS) 10, dado que IIS es un componente crítico para el funcionamiento de Exchange. Las acciones recomendadas incluyen:

Sistema Operativo:

a) Aplicación de guía de seguridad más moderna aplicable para IIS.

b) Deshabilitado de servicios innecesarios.

c) Configuración de auditoría avanzada para registro de eventos relevantes.

d) Verificación de instalación de los últimos parches de seguridad.

IIS:

a) Activación únicamente de los módulos requeridos por Exchange (deshabilitar módulos no utilizados).

b) Forzado de uso de protocolos seguros y deshabilitado de protocolos obsoletos.

c) Verificación de instalación de los últimos parches de seguridad.

Nota: para la correcta aplicación del procedimiento recogido en el presente documento, se asume que el entorno de implementación se encuentra formateado y con una aplicación de seguridad basada en CCN-STIC-570A25, tanto en el caso de una red clasificada, como en el caso del ENS.

5. PERFILADO DE CUMPLIMIENTO TÉCNICO

Antes de aplicar cualquier medida de seguridad específica sobre **Microsoft Exchange Subscription Edition,** es necesario implementar las medidas técnicas definidas por el ENS o ampliando el alcance del PCTE para entornos que manejan **Información Clasificada** mediante los requisitos de seguridad recogidos en la guía **CCN-STIC-570A25 Perfilado de Seguridad para Windows Server (DC o MS).**

Estas medidas, refuerzan la seguridad del Sistema Operativo Windows Server, proporcionando una base sólida y verificable sobre la que desplegar Exchange.

Por tanto, el perfil de aplicabilidad base, podrá ser:

a) ENS.

b) DIFUSIÓN LIMITADA.

c) Información Clasificada.

Con el objetivo de facilitar la implementación de la configuración de seguridad definida bajo el presente documento, en la próxima tablase recoge aquella agrupación de medidas de seguridad dependientes del grado de clasificación de la información y la categoría del sistema.

		CLASIFICACIÓN DE LA INFORMACIÓN/PERFIL		
		ENS	DIFUSIÓN LIMITADA	INFORMACIÓN CLASIFICADA
CATEGORÍA DEL SISTEMA DE INFORMACIÓN	BÁSICA	✓	✗	✗
	MEDIA	✓	✗	✗
	ALTA	✓	✗	✗
	DIFUSIÓN LIMITADA	✗	✓	✗
	CONFIDENCIAL RESERVADO SECRETO	✗	✗	✓

En los apartados siguientes se desarrollarán los controles específicos aplicables a Microsoft Exchange Subscription Edition, explicando su implementación técnica y las consideraciones específicas para entornos clasificados o de uso oficial. Solo tras aplicar estas medidas se procederá a la aplicación de seguridad específica de Microsoft Exchange Subscription Edition, garantizando una protección integral y alineada con la normativa vigente.

Nota: es posible obtener información sobre la interpretación de lo anteriormente comentado en el "Anexo II. Medidas de Seguridad" del ENS relativo a definición de medidas de seguridad.

- https://www.boe.es/buscar/doc.php?id=BOE-A-2022-7191

ANEXO A. Aplicación de Seguridad sobre Microsoft Exchange SE

En el presente anexo se define una marco base para la aplicación de aquellos requisitos de seguridad sobre el servicio Microsoft Exchange Subscription Edition, según los aspectos definidos en cada uno de los puntos anteriores de este documento.

Esta configuración se ofrece a modo de referencia o ejemplo de aplicabilidad de medidas en función de resultados concretos del análisis de riesgos ejecutado y en un entorno dirigido al tratamiento de Información Clasificada; es decir, el perfilado de medidas de seguridad expuestos a continuación, podría variar en el caso de otros escenarios y diferente superficie de exposición.

Nota: en caso de que el perfilado de seguridad y superficie de exposición obtenidos requieran de una configuración de seguridad avanzada, será necesario implementar medidas adicionales de seguridad. Por el contrario, en caso de que el resultado de dicho análisis indique que la necesidad de configuración solo deba establecerse según el perfilado básico, será posible evitar ciertas medidas de seguridad de las establecidas en el presente anexo.

Asimismo, ciertas categorías de seguridad no pueden ser aplicadas por medio de objetos GPO o configuraciones específicas a nivel de Windows AD DS, por ello se ha dedicado un apartado específico que permita establecer ejemplos de configuración sobre este tipo de categorías las cuales deberán ser adaptadas por cada organización.

Debe tenerse en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, se deberán realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y verificar el correcto funcionamiento del servicio y las configuraciones de seguridad aplicadas.

A modo de ejemplo, se procede a realizar un perfilado de seguridad aplicando a un servicio de Microsoft Exchange Server Subscription Edition. Previamente, se deben haber aplicado las configuraciones de seguridad necesarias sobre los servidores. A continuación, se especifican los servidores mínimos necesarios para proceder con el proceso de aplicación de seguridad:

- **Controlador de dominio:**
  - Sistema operativo: Windows Server 2025.
  - Nivel funcional del dominio: Windows Server 2016.
  - Guía base de aplicación de seguridad utilizada: CCN-STIC-570A25. Perfilado de seguridad para Windows Server (DC o MS).
- **Servidores Exchange Server Subscription Edition** (2 servidores):
  - Sistema operativo: Windows Server 2025.
  - Guía base de aplicación de seguridad utilizada: CCN-STIC-570A25. Perfilado de seguridad para Windows Server (DC o MS).
  - Guía específica de aplicativo IIS.
- **Entidad certificadora** (1 servidor):
  - Sistema operativo: Windows Server 2025.

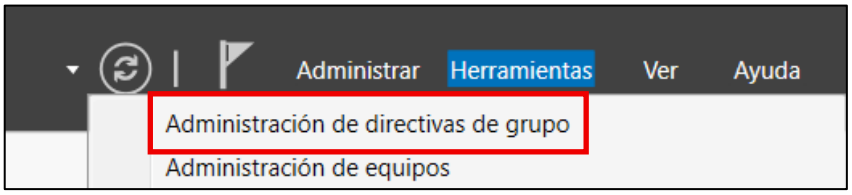
- Guía base de aplicación de seguridad utilizada:
  - CCN-STIC sobre Implementación de seguridad en Entidad de Certificación sobre Windows Server.
  - CCN-STIC-574A25 Implementación de Seguridad en Internet Information Services 10 sobre Microsoft Windows Server 2016.
  - CCN-STIC-570A25. Perfilado de seguridad para Windows Server (DC o MS).

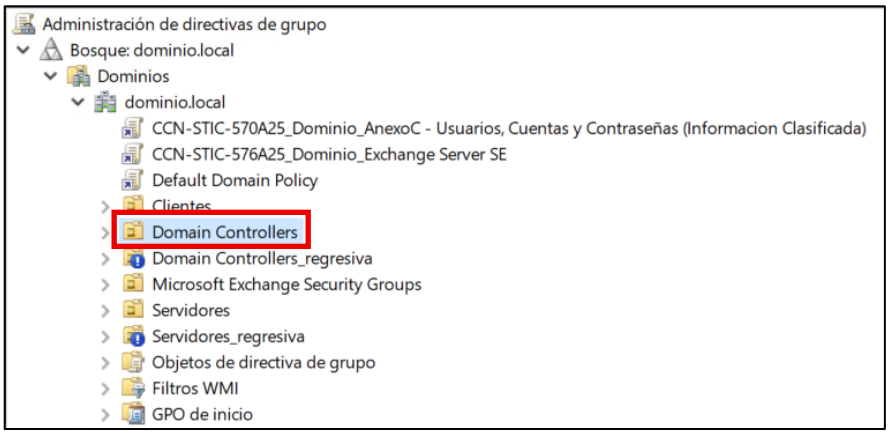
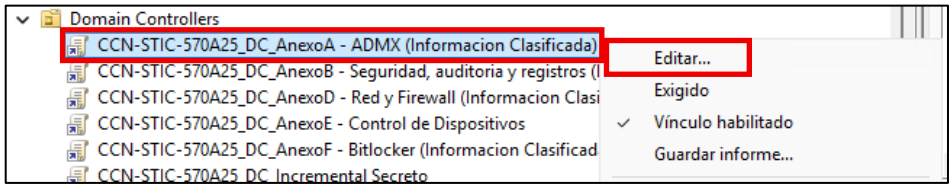
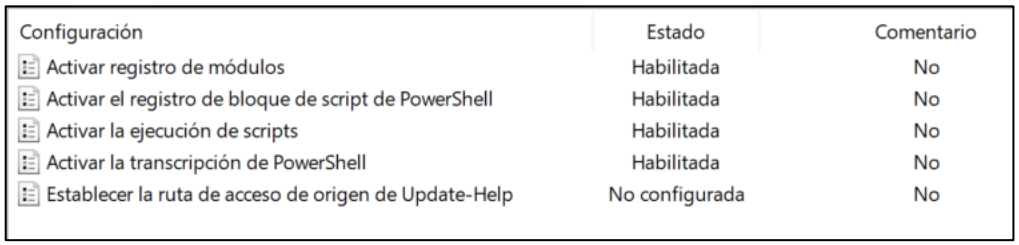
Nota: es importante destacar que las guías de seguridad mencionadas han sido aplicadas sobre los servidores involucrados, tras la completa configuración del servicio de Exchange Server Subscription Edition. Asimismo, es importante aclarar que, en el momento de la redacción de la presente guía, los DCs pueden disponer desistema operativo Windows Server 2025, mientras que Exchange Server Subscription Edition no es compatible con el nivel funcional de dominio de Windows Server 2025. Así, es necesario planificar el dominio para utilizar nivel funcional de bosque Windows Server 2016.

El usuario administrador del dominio que se utilice para todas las tareas descritas en la presente operativa deberá pertenecer a los siguientes grupos:

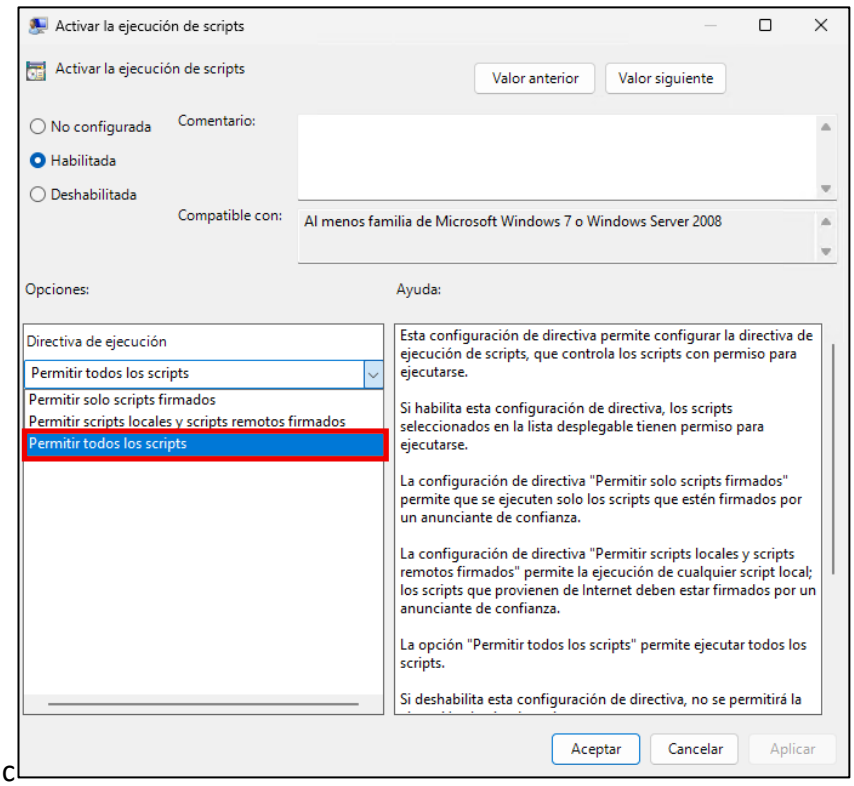
- Administradores.
- Administradores de empresas.
- Administradores de esquema.
- Admins. de dominio.
- Organization Manager.
- Propietarios del creador de directivas de grupo.
- Usuarios del dominio.

ANEXO A.1. Implementación de Políticas de Seguridad sobre el Dominio

Paso	Descripción
1.	Inicie sesión con un usuario miembro del grupo Admins. de Dominio en un Controlador de Dominio.
2.	En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.  *Ilustración 1 - Administración de directivas de grupo*

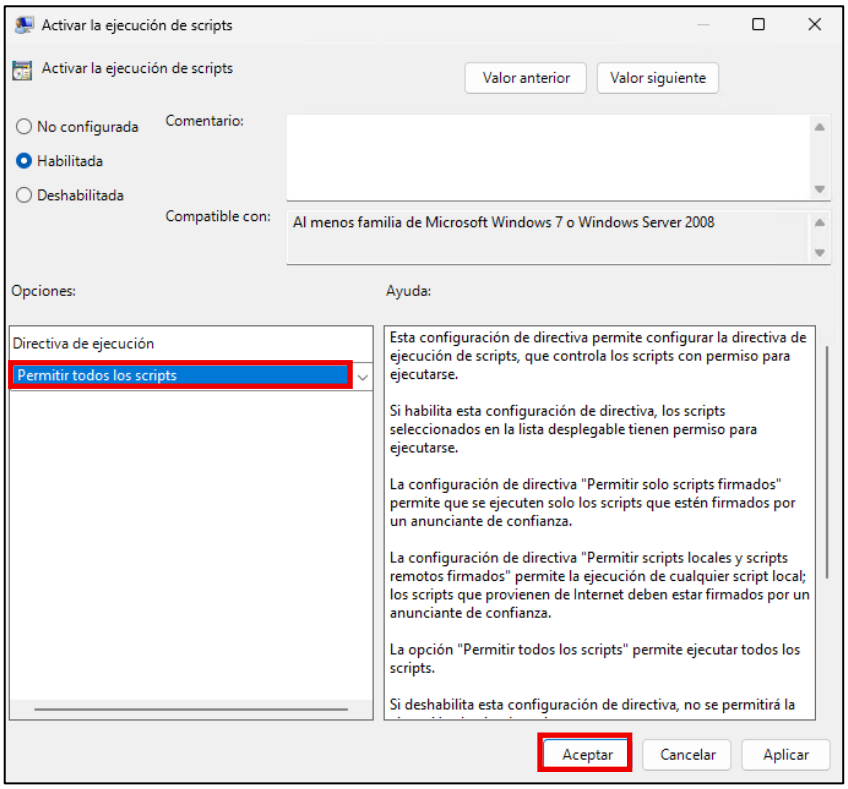
3.	Despliegue en el panel izquierdo hasta llegar a la OU “Domain Controllers”.  *Ilustración 2 - OU Domain Controllers*
4.	Despliegue dicha Unidad Organizativa, haga clic derecho sobre el GPO “CCN-STIC-570A25_DC_AnexoA – ADMX (Nivel de Clasificación)”, y seleccione “Editar”.  *Ilustración 3 - Edición de ADMX 570A25*
5.	En el panel “Editor de administración de directivas de grupo”, despliegue la lista siguiendo la siguiente ruta: “Configuración del Equipo > Plantillas administrativas > Componentes de Windows > Windows PowerShell”. Haga clic sobre “Windows PowerShell” para consultar las políticas que aplica.  *Ilustración 4 - Políticas de PowerShell*
6.	Haga doble clic sobre la política “Activar la ejecución de scripts”.

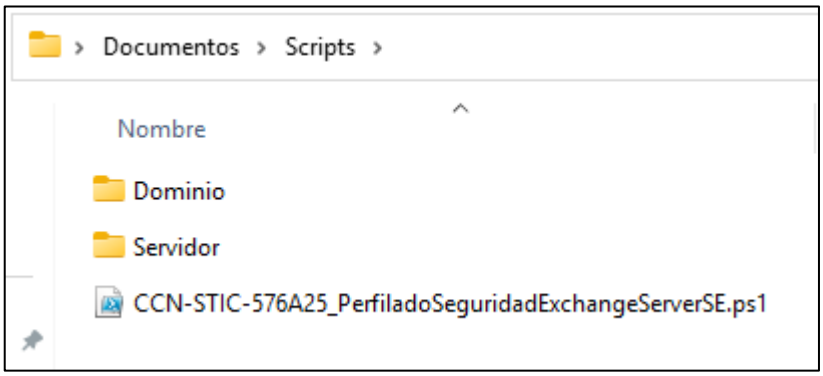
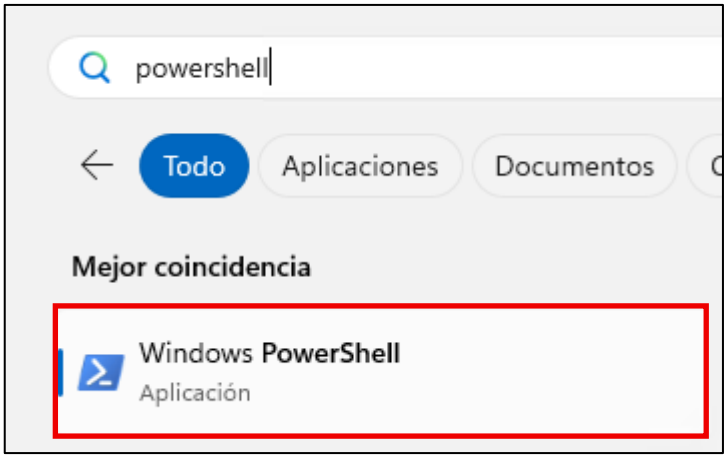
7. En el desplegable de la política, seleccione “Permitir todos los scripts”, y haga clic en “Aplicar” y “Aceptar”.

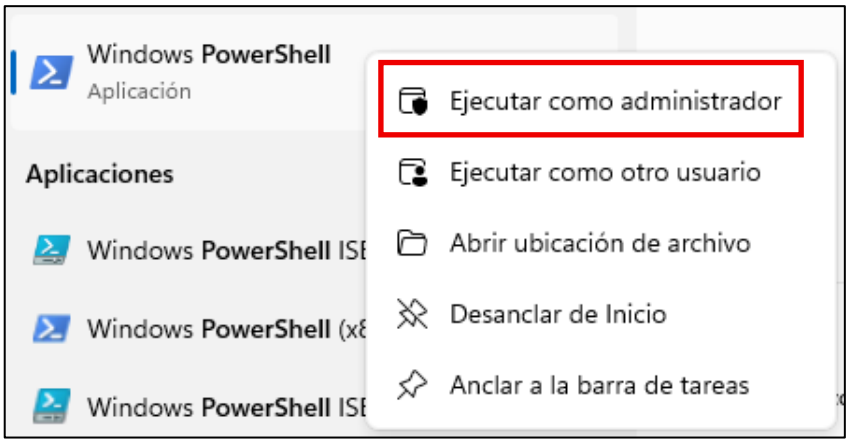
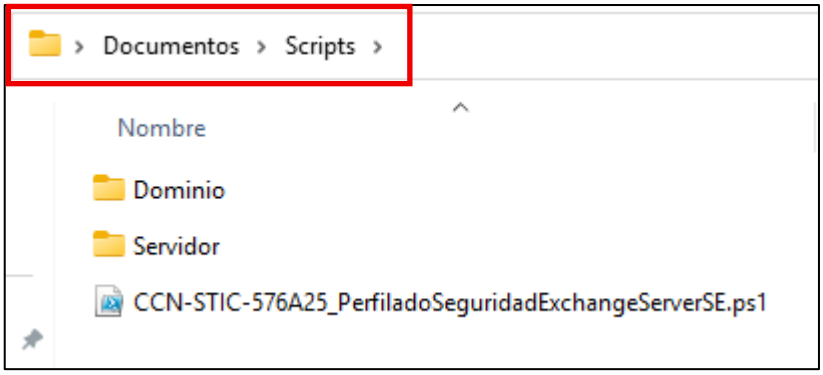


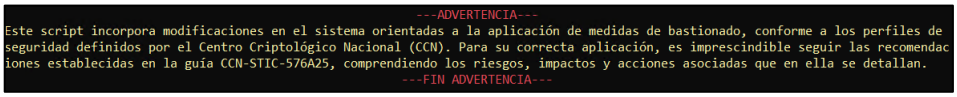
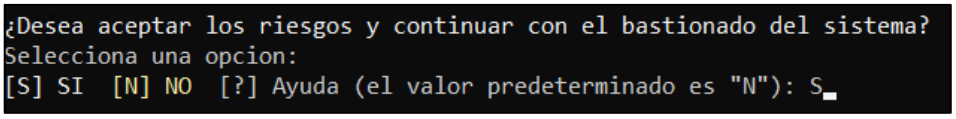
c

Ilustración 5 - Selección de "Permitir todos los scripts"



8.	Reinicie el controlador de dominio para que se aplique la configuración correctamente.
9.	Copie los ficheros y directorios que acompañan a esta guía al directorio en la carpeta "Documentos" del usuario administrador. A continuación, descomprima la carpeta. Verifique que en su interior se encuentran los siguientes archivos: - Directorio: Dominio - Directorio: Servidor - Fichero: CCN-STIC-576A25_PerfiladoSeguridadExchangeServerSE.ps1  *Ilustración 6 - Copia de ficheros necesarios*
10.	Sobre la barra de búsqueda, escriba "PowerShell":  *Ilustración 7 - Windows PowerShell*

11.	Haga clic derecho, y seleccione “Ejecutar como administrador”:  *Ilustración 8 - Ejecución como administrador* **Nota:** Si el script no se ejecuta desde PowerShell, existe la posibilidad de que ocurran fallos durante el proceso de copia y/o que no se visualice la información de manera adecuada.
12.	Desde el explorador de archivos, acceda al contenido de carpeta en la que ha copiado los scripts y copie la ruta en el portapapeles con “Ctrl + C”.  *Ilustración 9 - Copia de ruta*
13.	Desde la ventana de PowerShell, utilizando el comando “cd”, acceda a la ruta recientemente copiada.  *Ilustración 10 - Acceso a la ruta*

14.	Ejecute el comando “dir” para verificar la ubicación y el contenido.  *Ilustración 11 - Contenido de la carpeta*
15.	Ejecute el archivo “CCN-STIC576A25_PerfiladoSeguridadExchangeServerSE.ps1” escribiendo “.\” y pulsando la tecla tabuladora hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución.  *Ilustración 12 - Ejecución del script*
16.	A continuación, se mostrará una advertencia de uso, continuando con el siguiente mensaje:  *Ilustración 13 - Advertencia*
17.	Escribir “S” y pulsar “Enter”.  *Ilustración 14 - Aceptación de advertencia*
18.	Aparecerán dos opciones de configuración: - [D] Configuración de dominio - [E] Configuración del servidor de Exchange SE Escribir “D” y pulsar “Enter” para completar la configuración de dominio.  *Ilustración 15 - Selección de configuración*
19.	Espere a que termine la ejecución. Una vez hecho, deberá escribir “S” y pulsar “Enter” para continuar con la configuración.

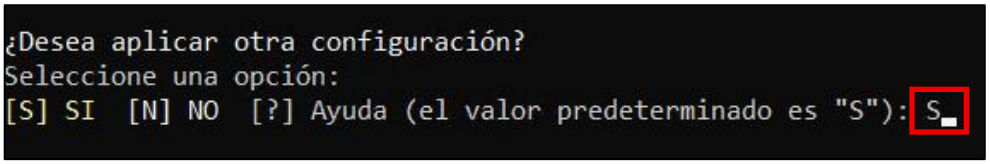


Ilustración 16 - Aplicación de otra configuración

20. Para aplicar la configuración del servidor en el que está instalado Exchange Server SE, deberá escribir “E” y pulsar “Enter”.

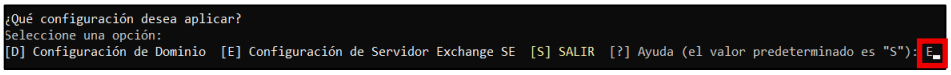
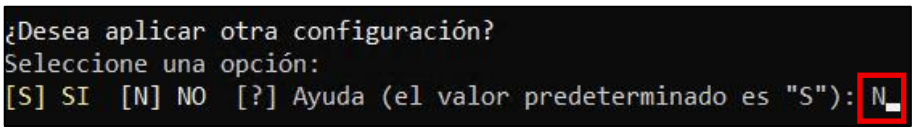


Ilustración 17 - Selección de configuración

21. Para salir del script, escriba “N” y pulse “Enter” en la última petición de confirmación.



22. En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.

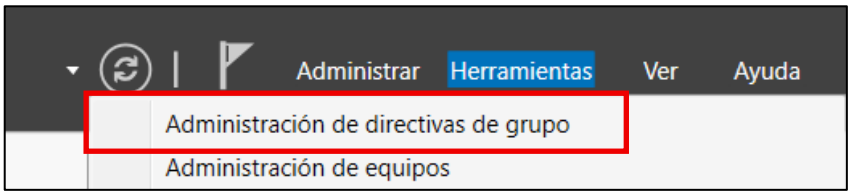


Ilustración 18 - Administración de directivas de grupo

23. Expanda la lista del menú izquierdo hasta llegar al dominio, y haga clic sobre él para seleccionarlo.

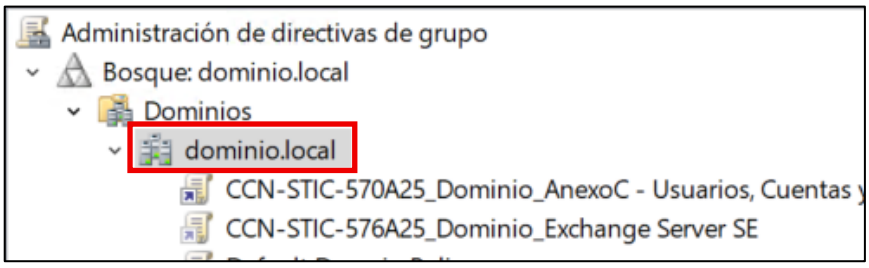
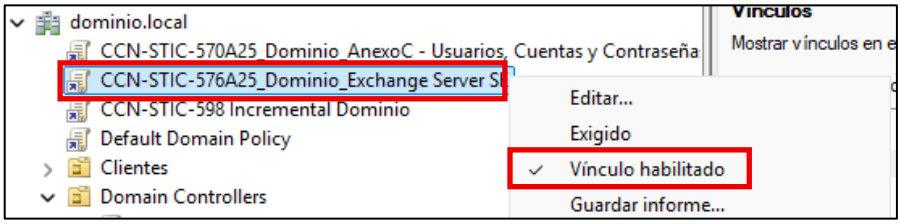
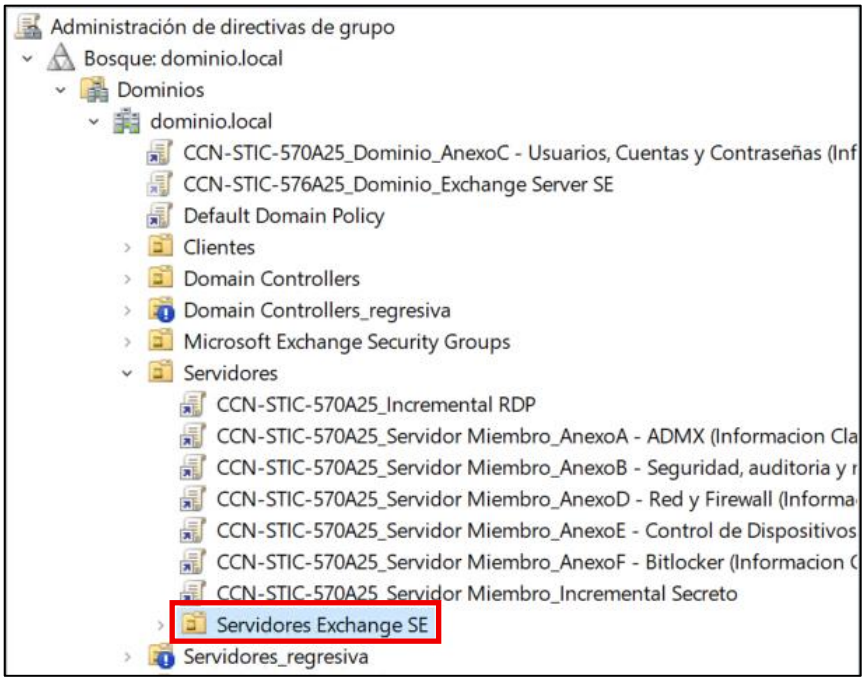
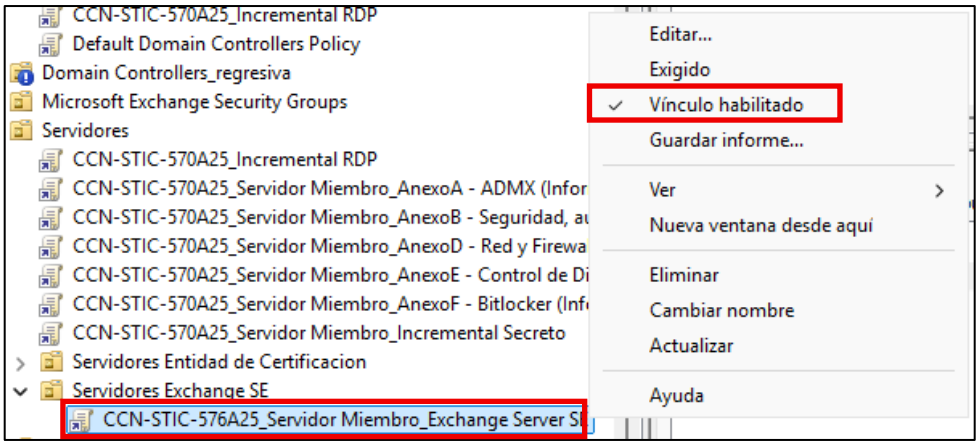
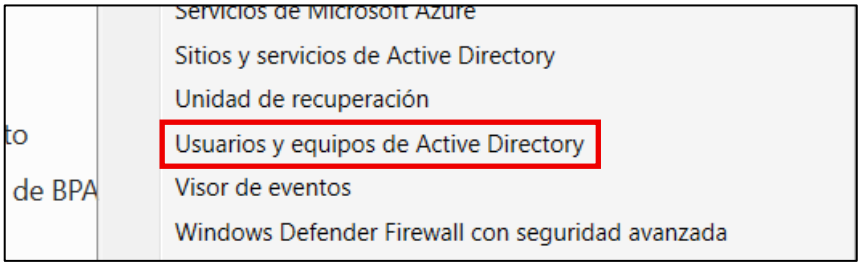
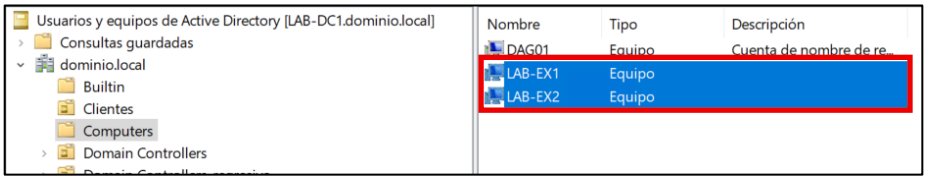


Ilustración 19 - Selección del dominio

24.	En el panel derecho, diríjase a la pestaña “Objetos de directiva de grupo vinculados”, y asegúrese de que el orden de GPOs es el siguiente:  *Ilustración 20 - Orden de los GPOs*
25.	De nuevo en el panel izquierdo, haga clic derecho sobre el GPO “CCN-STIC-576A25_Dominio_Exchange Server SE”, y seleccione la opción “Vínculo habilitado” para vincular dicho GPO y que se haga efectivo.  *Ilustración 21 – Habilitación del vínculo*
26.	En el panel izquierdo, despliegue la OU “Servidores”, y dentro, haga clic sobre la OU “Servidores Exchange SE” recientemente creada para seleccionarla.  *Ilustración 22 - OU Servidores Exchange SE*

27.	Despliegue dicha OU y haga clic derecho sobre el GPO "CCN-STIC-576A25_Servidor Miembro_Exchange Server SE". Seleccione la opción "Vínculo habilitado".  *Ilustración 23 - Habilitación de vínculo*
28.	De nuevo en el "Administrador del servidor", haga clic en "Herramientas" en la barra superior, y seleccione "Usuarios y equipos de Active Directory".  *Ilustración 24 - Usuarios y equipos de Active Directory*

29.	Despliegue la lista del panel izquierdo hasta visualizar la OU “Servidores Exchange SE”.  *Ilustración 25 - OU Servidores Exchange SE*
30.	Haga clic sobre la carpeta “Computers” y seleccione los dos servidores de Exchange Server SE.  *Ilustración 26 - Selección de los servidores*
31.	Arrástrelos a la OU “Servidores Exchange SE”. Aparecerá una advertencia. Haga clic en “Sí”.
32.	A continuación, reinicie uno a uno los controladores de dominio para que se les aplique el GPO de Dominio. Una vez hecho, reinicie los servidores Exchange Server SE para que se les apliquen los GPOs de Dominio de Servidor.
33.	Inicie sesión con el usuario con el que se configuró Exchange en uno de los servidores que alojan el servicio Exchange Server SE.

34.	Sobre la barra de búsqueda, escriba “Exchange Management Shell”.

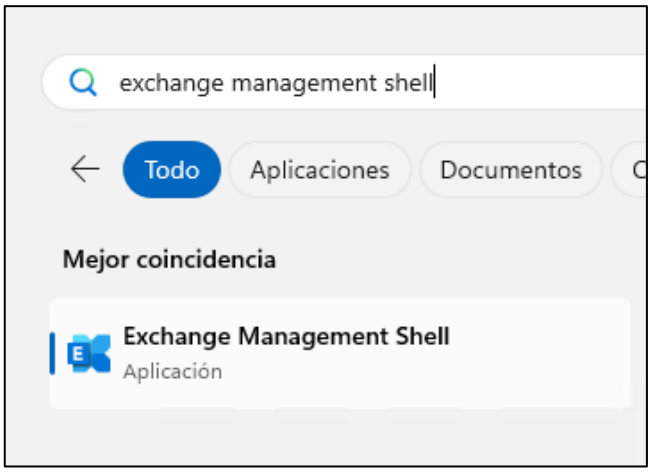


Ilustración 27 - Exchange Management Shell

35.	Haga clic derecho y seleccione “Ejecutar como administrador”.

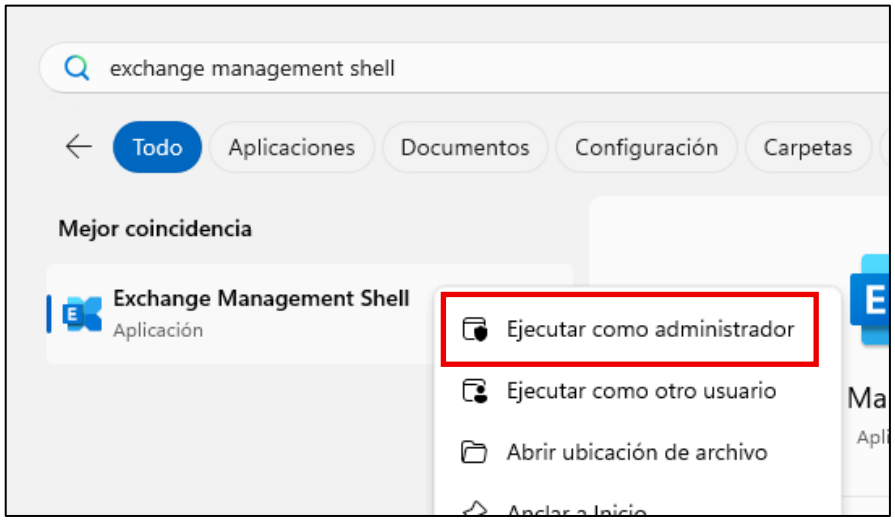


Ilustración 28 - Ejecución como administrador

36.	Espere a que cargue la consola y aparezca una advertencia. Entonces, copie la ruta al archivo indicado:

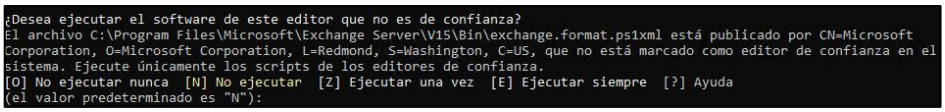
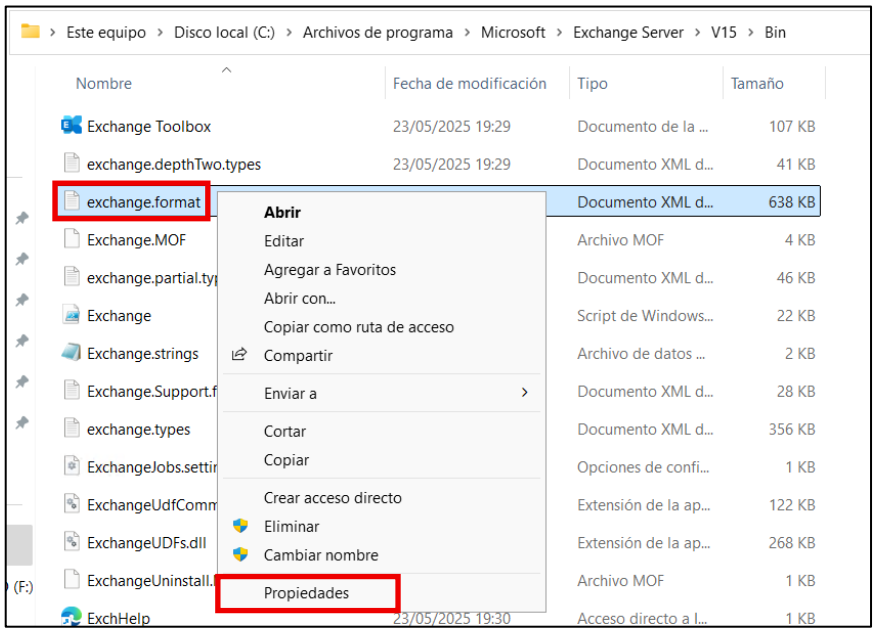
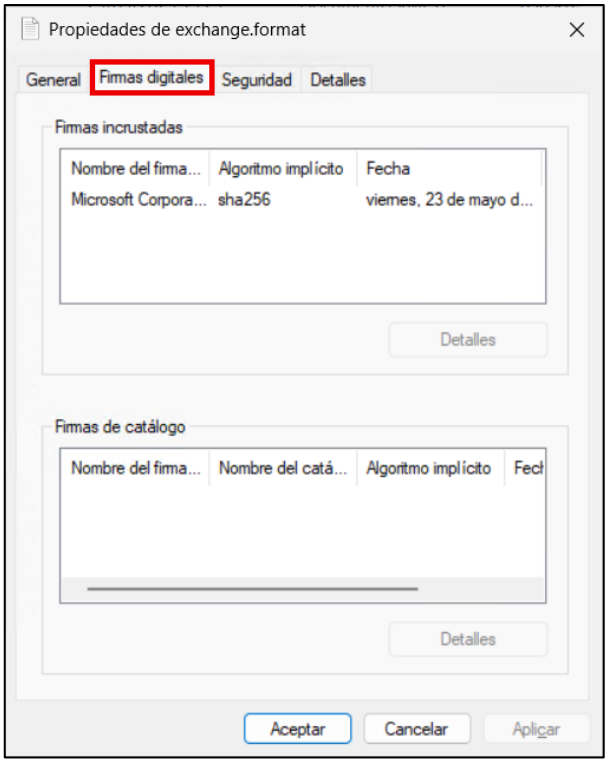


Ilustración 29 - Copia de la ruta

En este caso, sería “C:\Program Files\Microsoft\Exchange Server\V15\Bin\exchange.format.ps1xml”.

Nota: la ruta será diferente si se seleccionó un directorio distinto durante la instalación.

37.	Cierre la consola de “Exchange Management Shell”.
38.	En el explorador de archivos, diríjase a la ruta recogida anteriormente, haga clic derecho sobre el archivo en cuestión y seleccione “Propiedades”.  *Ilustración 30 - Propiedades del archivo*
39.	Diríjase a la pestaña “Firmas digitales”.  *Ilustración 31 - Firmas digitales*

40.	Seleccione la firma que aparece y haga clic en “Detalles”.

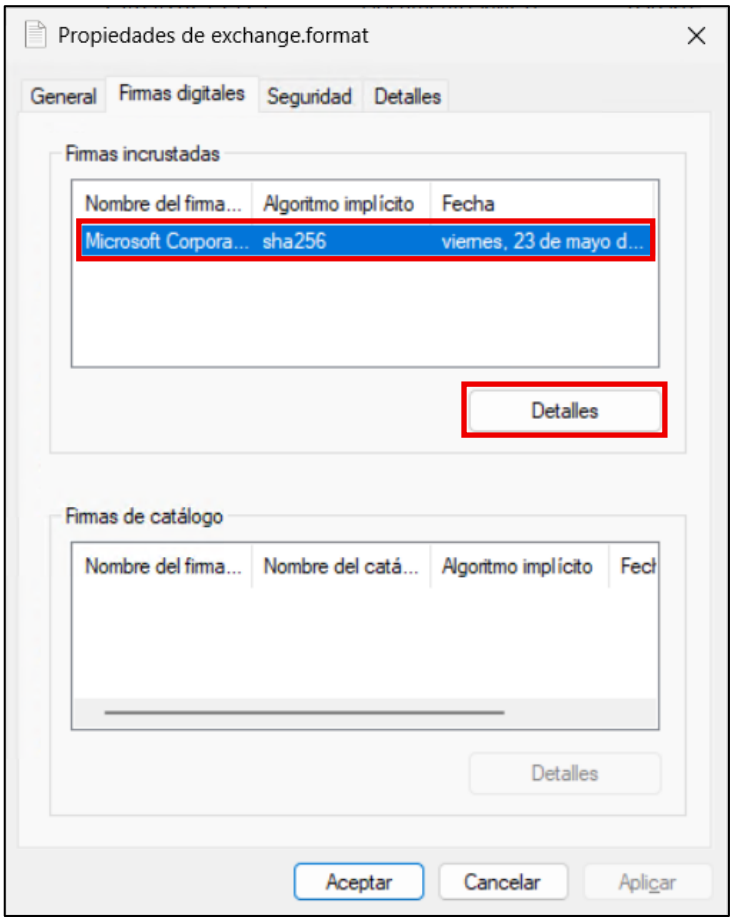


Ilustración 32 - Detalles del certificado

41.	En la ventana que se abra, haga clic en “Ver certificado”.

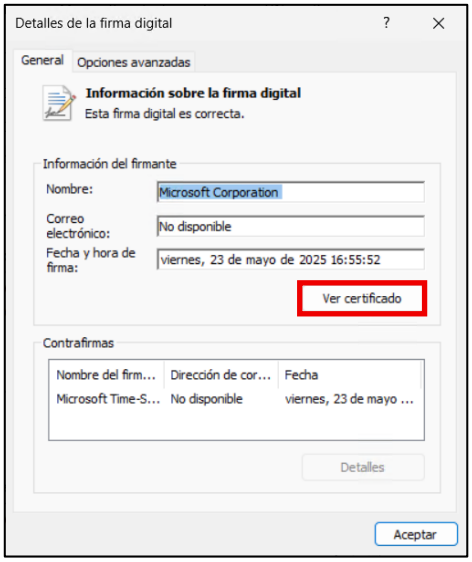
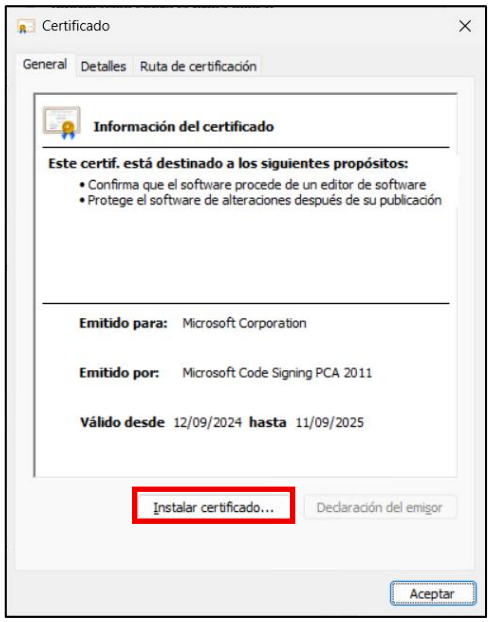
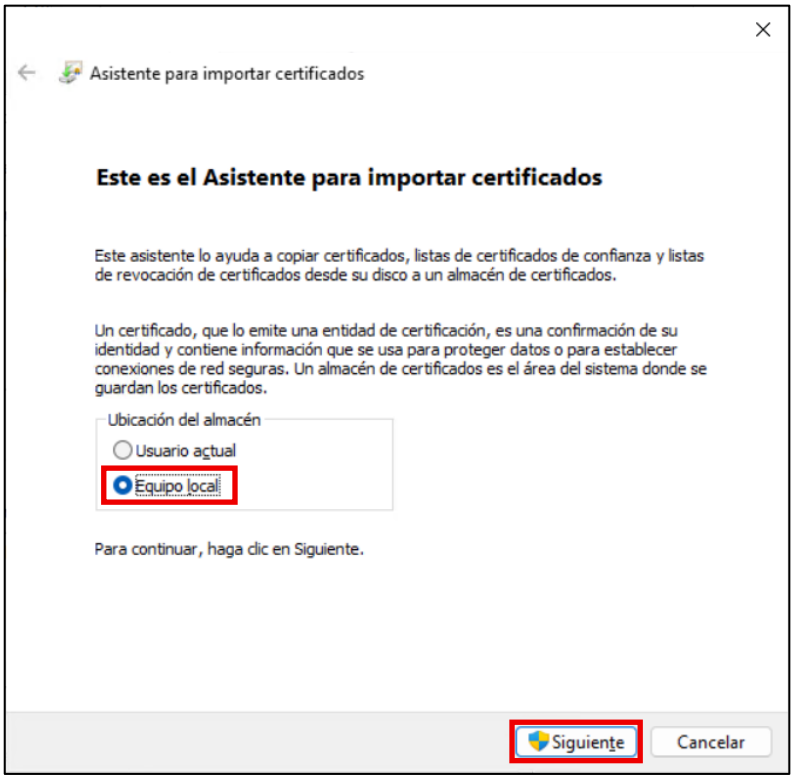


Ilustración 33 - Visualización del certificado

42.	En la ventana que se abra, haga clic en “Instalar certificado”.  *Ilustración 34 - Instalación del certificado*
43.	Seleccione “Equipo local”. Haga clic en “Siguiente” e introduzca sus credenciales de administrador.  *Ilustración 35 - Selección de equipo local*

44.	Seleccione “Colocar los certificados en el siguiente almacén”, y haga clic en “Examinar”.

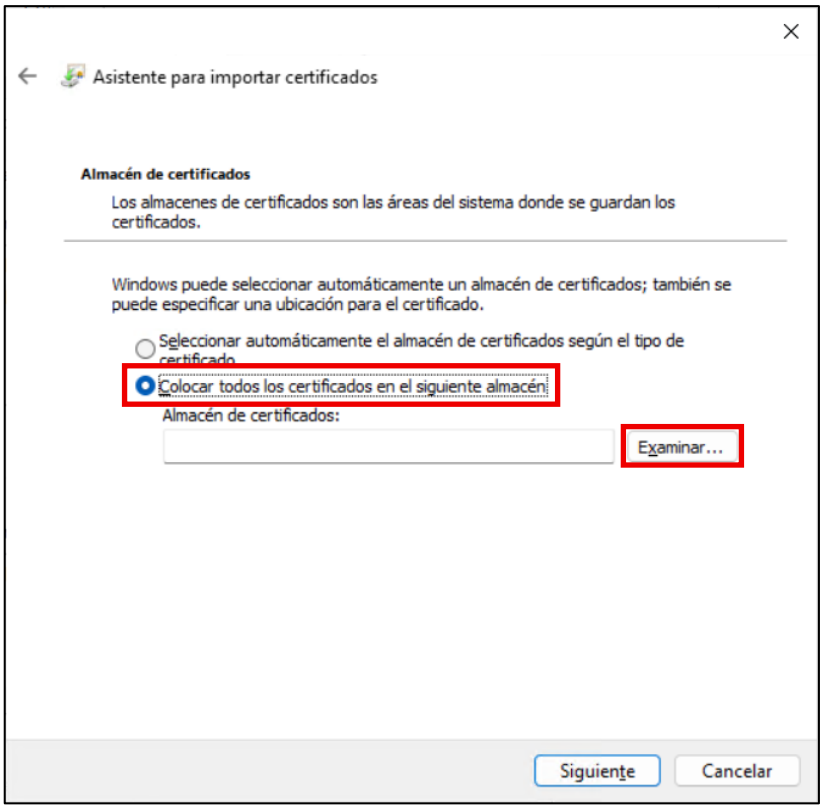


Ilustración 36 - Selección del almacén de certificados

45.	Seleccione el almacén “Editores de confianza” y haga clic en “Aceptar”.

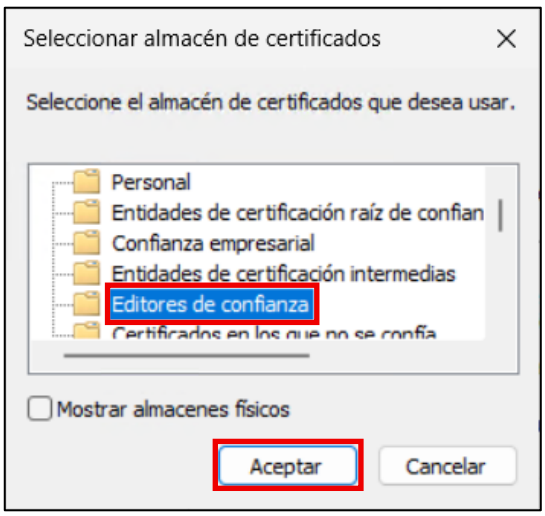


Ilustración 37 - Almacén "Editores de confianza"

46.	Haga clic en “Siguiente”.

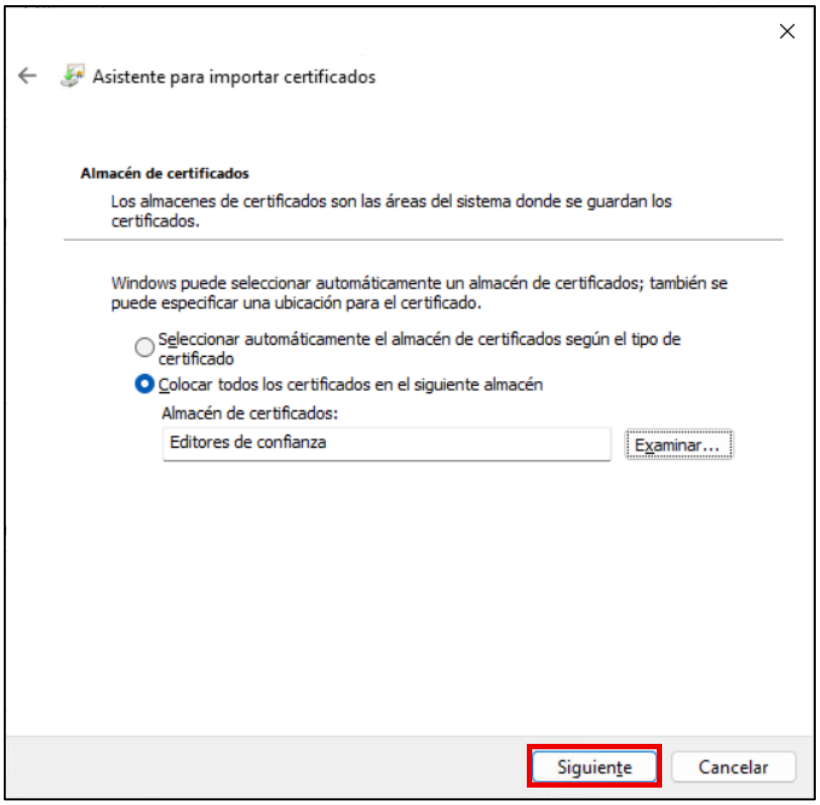


Ilustración 38 - Confirmación del almacén

47.	Haga clic en “Finalizar”.

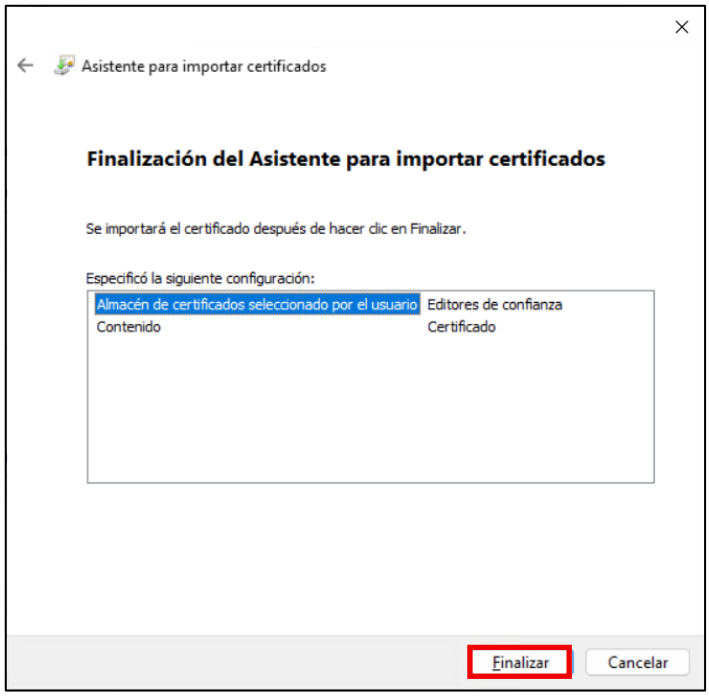
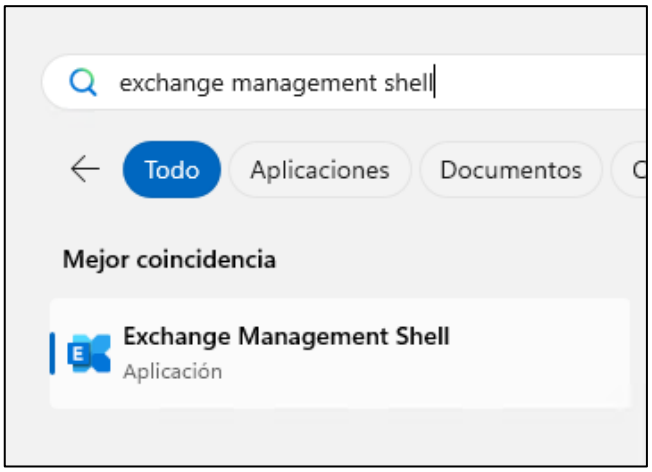
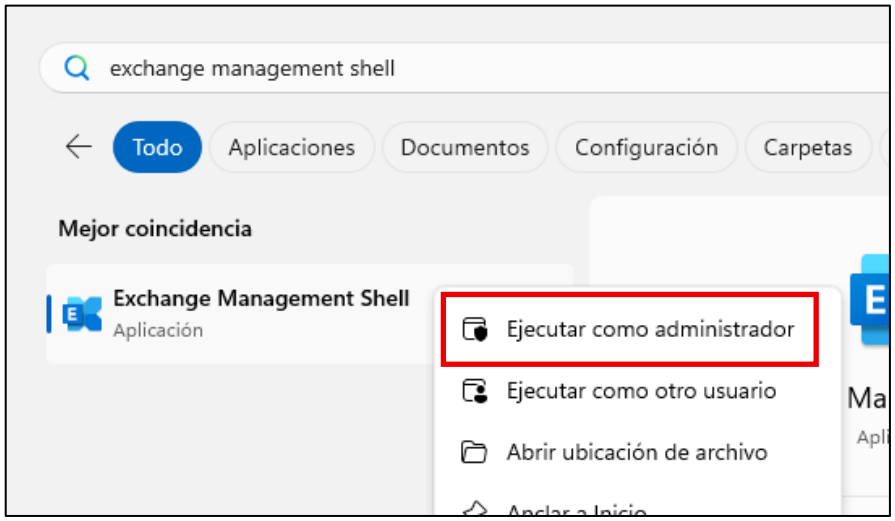
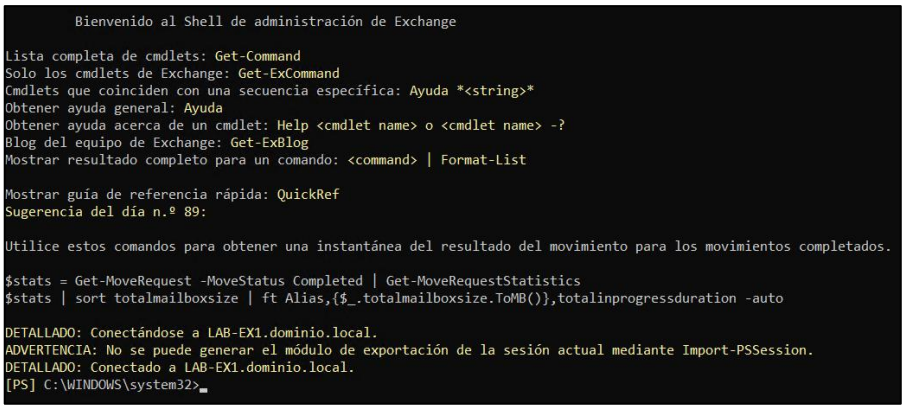
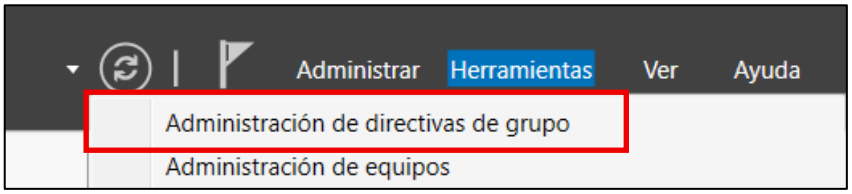
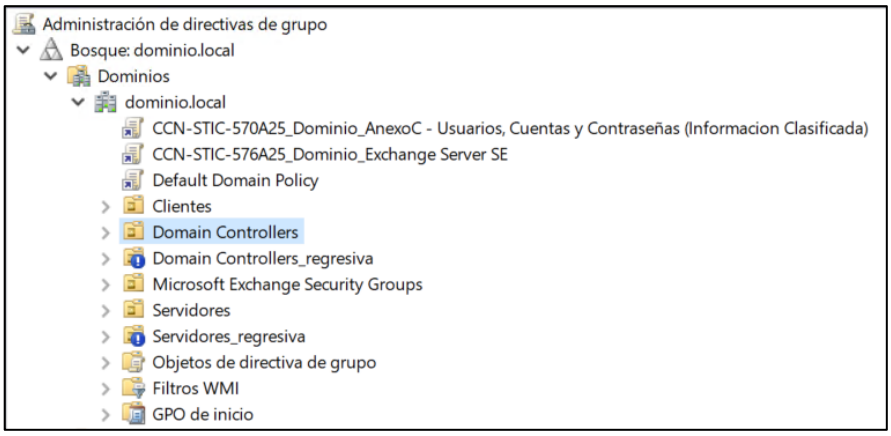
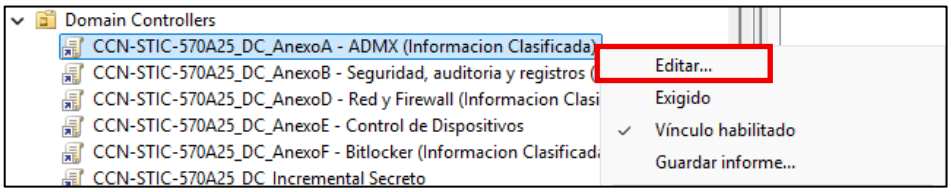
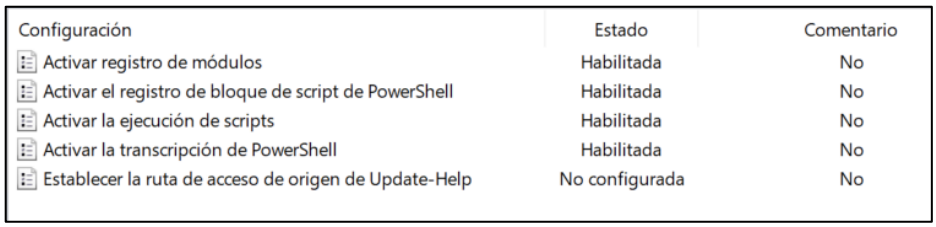


Ilustración 39 - Finalización de la configuración

48.	Sobre la barra de búsqueda, escriba “Exchange Management Shell”.  *Ilustración 40 - Exchange Management Shell*
49.	Haga clic derecho y seleccione “Ejecutar como administrador”.  *Ilustración 41 - Ejecución como administrador*

50.	Verificar que no aparece ninguna advertencia y que inicia la consola sin interrupciones.  *Ilustración 42 - Confirmación del correcto funcionamiento*
51.	Repetir el mismo proceso en el resto de los servidores de Exchange Server SE: **Nota:** A partir de este momento, siempre que se abra "Exchange Management Shell" en los servidores de Exchange, será necesario introducir el siguiente comando para poder utilizar todas las funciones: > Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn -ErrorAction SilentlyContinue
52.	Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en un Controlador de Dominio.
53.	En el "Administrador del servidor", haga clic en "Herramientas" en la barra superior y seleccione "Administración de directivas de grupo".  *Ilustración 43 - Administración de directivas de grupo*

54.	Despliegue el panel izquierdo hasta llegar a la OU “Domain Controllers”.  *Ilustración 44 - OU Domain Controllers*
55.	Despliegue dicha OU, haga clic derecho sobre el GPO “CCN-STIC-570A25_DC_AnexoA – ADMX (Nivel de Clasificación)”, y seleccione “Editar”.  *Ilustración 45 - Edición ADMX 257A25*
56.	En el panel izquierdo, despliegue la lista siguiendo la siguiente ruta: “Configuración del Equipo > Plantillas administrativas > Componentes de Windows > Windows PowerShell”. Haga clic sobre “Windows PowerShell” para ver las políticas que aplica  *Ilustración 46 - Políticas de PowerShell*
57.	Haga doble clic sobre la política “Activar la ejecución de scripts”.

58.	En el desplegable de la política, seleccione “Permitir solo scripts firmados”, y haga clic en “Aplicar” y “Aceptar”.
59.	Reinicie el controlador de dominio para que se aplique la configuración correctamente.

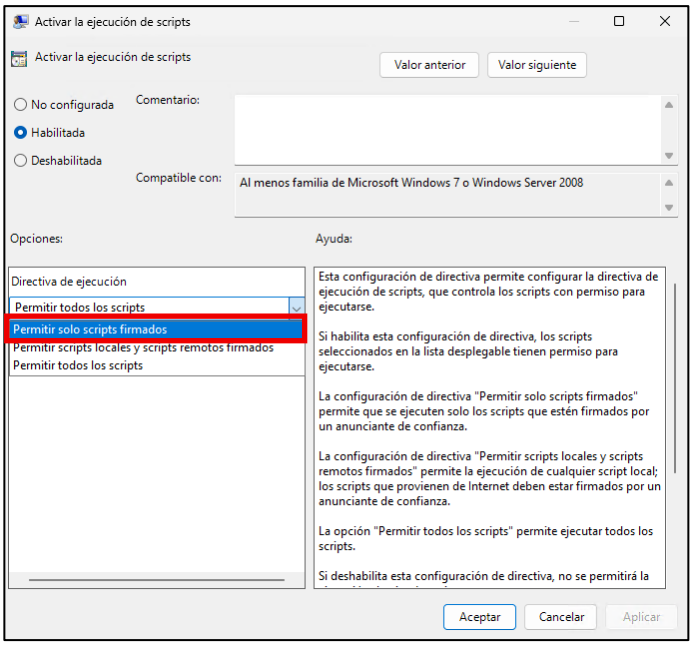


Ilustración 47 - Selección de "Permitir solo scripts firmados"

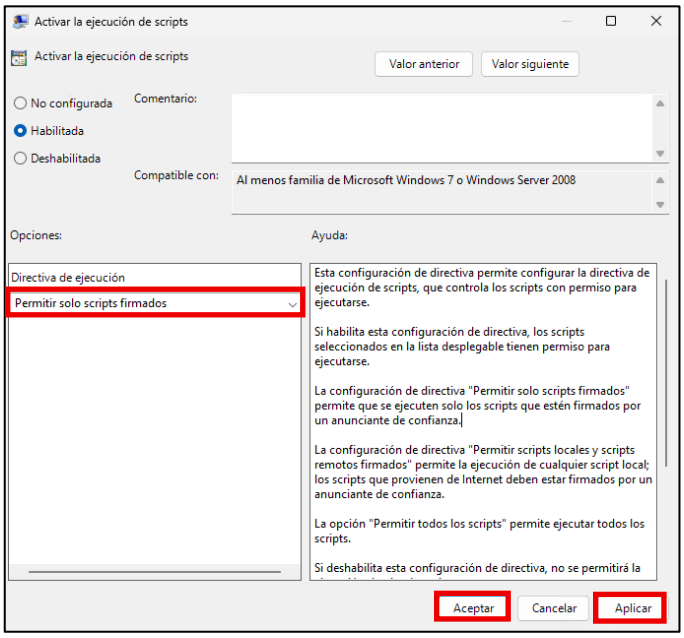


Ilustración 48 - Aplicación de la política

ANEXO A.2. Configuraciones Adicionales

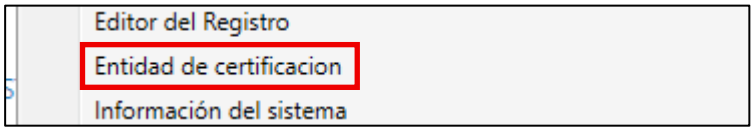
El presente apartado recoge aquellas categorías de perfilado de seguridad asociadas a un riesgo concreto las cuales no pueden ser aplicadas por medio de configuraciones a nivel de Windows, al depender del entorno en el que vaya a realizarse la aplicación del perfilado de seguridad. Esto puede deberse a diversos factores, entre ellos, el uso de otro software que realiza la misma función o bien debido a que se establecen las medidas que evitan el riesgo por medio otros parámetros y/o configuraciones.

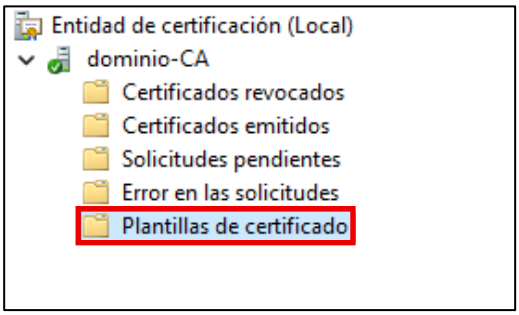
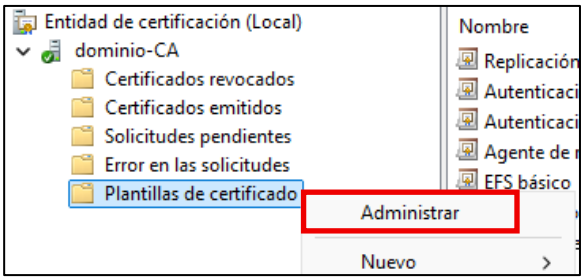
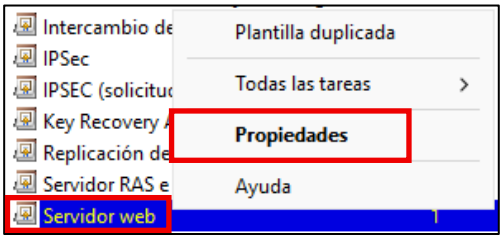
Para estos casos, se desarrolla el presente anexo, en el cual se establecen comentarios sobre las categorías de perfilado de seguridad de nivel intermedio afectadas y se determina un ejemplo de configuración o validación que permita garantizar el aseguramiento de Microsoft Exchange Server SE con la premisa de apoyar a los operadores a realizar un correcto aseguramiento.

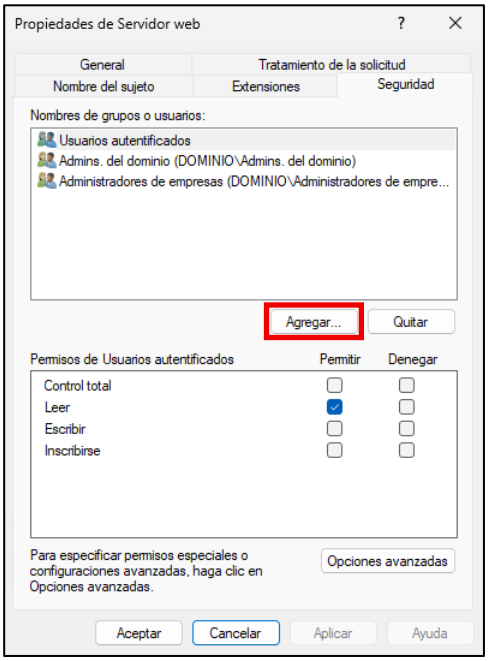
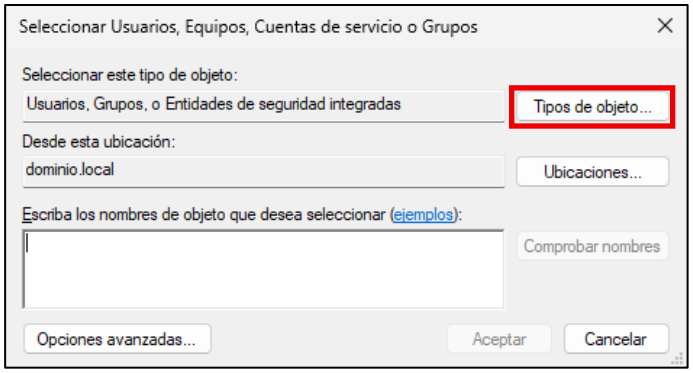
Nota: las diferentes configuraciones ofrecidas en este anexo son una referencia de las múltiples soluciones que se pueden encontrar para cada uno de los riesgos identificados, es decir, la misma funcionalidad aquí presentada para la mitigación del riesgo puede ser aplicada mediante otros procedimientos, software, o configuraciones. No deben tomarse estas configuraciones como métodos únicos de mitigación.

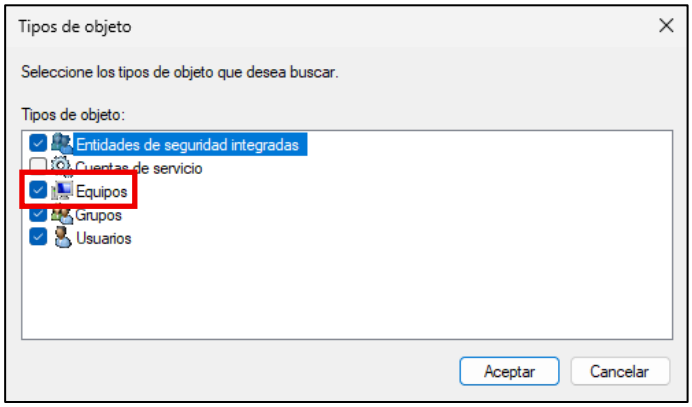
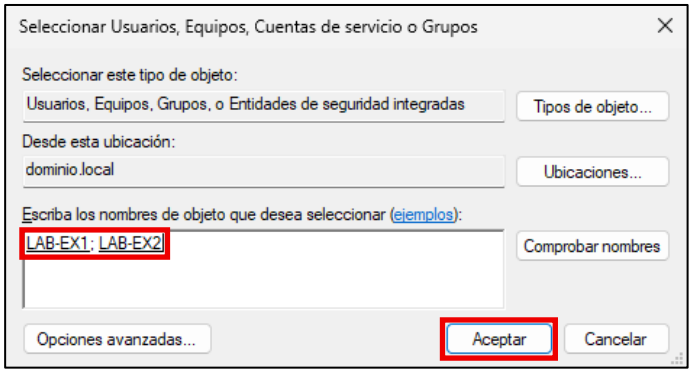
ANEXO A.2.1. Configuración de Certificados

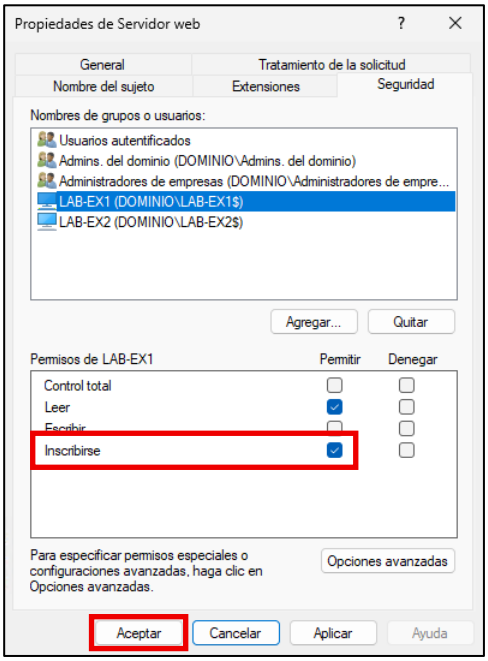
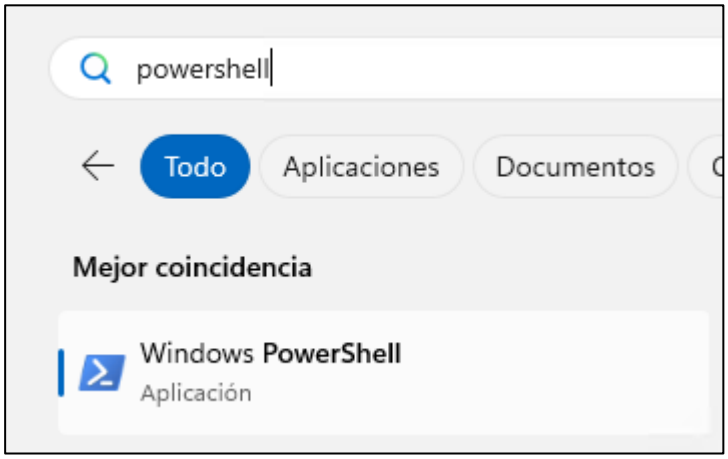
A Continuación, se muestra un ejemplo de cómo realizar la solicitud e instalación de certificados correspondiente mediante solicitud sin conexión. Si bien es cierto que en algunos escenarios se puede realizar mediante solicitud a entidad de certificación “Enterprise”, se realiza mediante el método sin conexión para que el procedimiento resulte funcional en cualquiera de los casos.

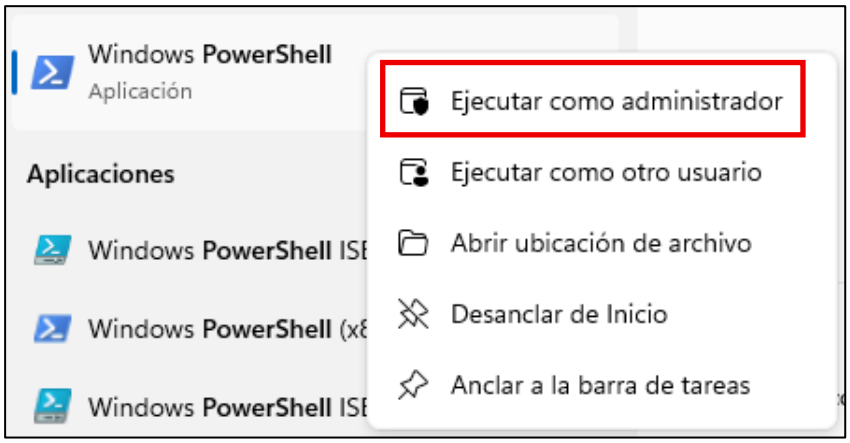
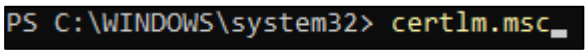
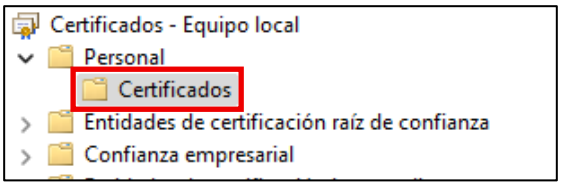
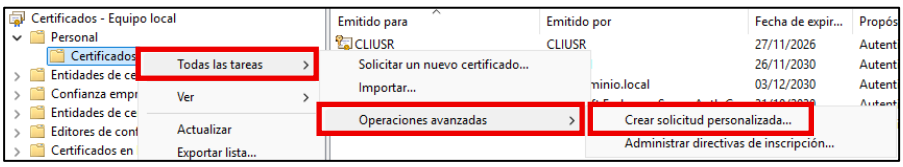
Paso	Descripción
1.	Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en el servidor Entidad de Certificación
2.	En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Entidad de certificación”.  *Ilustración 49 - Entidad de certificación*

3.	Despliegue la lista del panel lateral izquierdo hasta llegar a “Plantillas de certificado”.  *Ilustración 50 - Plantillas de certificado*
4.	Haga clic derecho sobre “Plantillas de certificado” y seleccione “Administrar”.  *Ilustración 51 - Administración de plantillas de certificado*
5.	Busque “Servidor web” en la lista, haga clic derecho sobre dicho elemento y seleccione “Propiedades”.  *Ilustración 52 - Propiedades de la plantilla*

6.	Diríjase a la pestaña “Seguridad”, y haga clic sobre “Agregar”.  *Ilustración 53 - Adición de elementos*
7.	Haga clic sobre “Tipos de objeto”.  *Ilustración 54 - Tipos de objeto*

8.	Marque la casilla “Equipos” y haga clic en “Aceptar”.  *Ilustración 55 - Selección de "Equipos"*
9.	Introduzca los nombres de los dos servidores de Exchange y haga clic en “Aceptar”.  *Ilustración 56 - Aplicación de la selección*

10.	Marque la casilla “Inscribirse” y haga clic en “Aceptar”.  *Ilustración 57 - Habilitación de permiso para inscripción*
11.	Inicie sesión con el usuario con el que se configuró Exchange en uno de los servidores que alojan el servicio Exchange Server SE.
12.	Sobre la barra de búsqueda, escriba “PowerShell”.  *Ilustración 58 - Windows PowerShell*

13.	Haga clic derecho, y seleccione “Ejecutar como administrador”.  *Ilustración 59 - Ejecución como administrador*
14.	Abra el administrador de certificados de máquina.  *Ilustración 60 - Ejecución de “certlm.msc”*
15.	Despliegue la lista del panel izquierdo hasta llegar a “Personal > Certificados”.  *Ilustración 61 - Certificados*
16.	Haga clic derecho sobre “Certificados” y seleccione “Todas las tareas > Operaciones avanzadas > Crear solicitud personalizada”.  *Ilustración 62 - Creación de solicitud personalizada*

17. Haga clic en “Siguiente”.

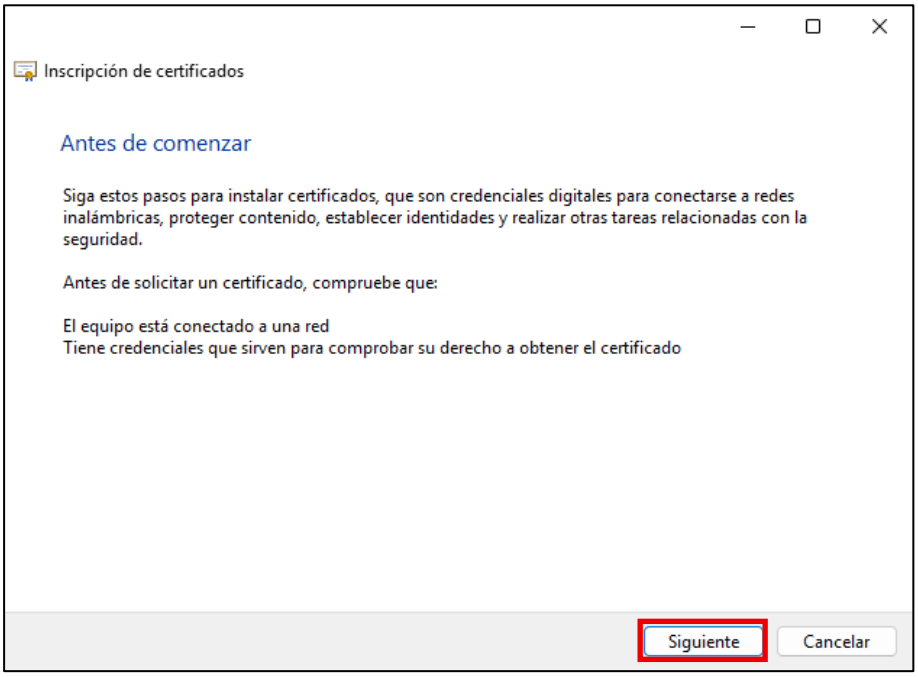


Ilustración 63 - Solicitud personalizada

18. Haga clic en “Siguiente”.

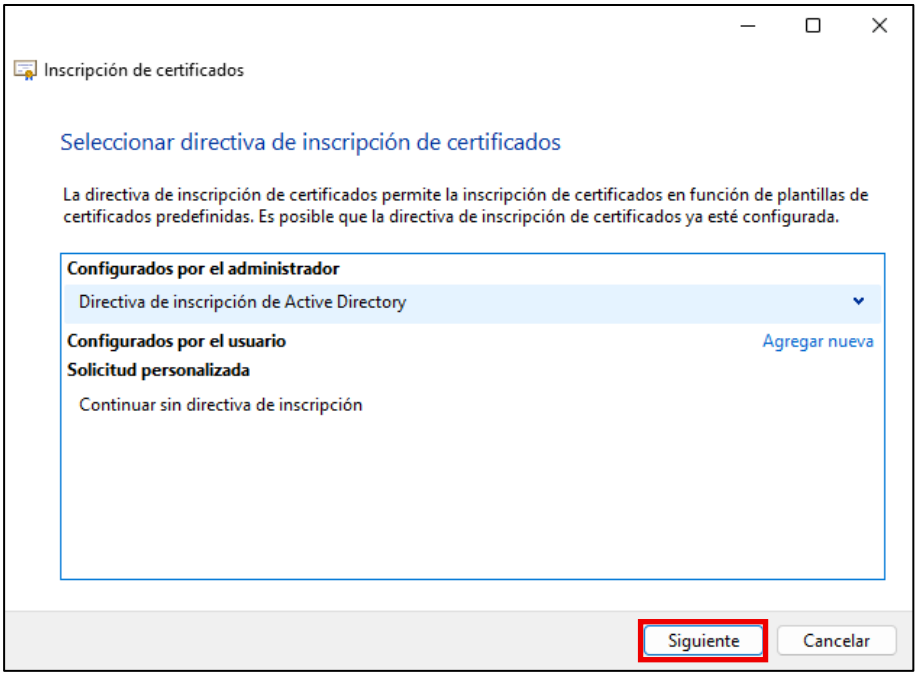


Ilustración 64 - Solicitud personalizada

19.	En la lista desplegable, seleccione “Servidor web” y haga clic en “Siguiente”.

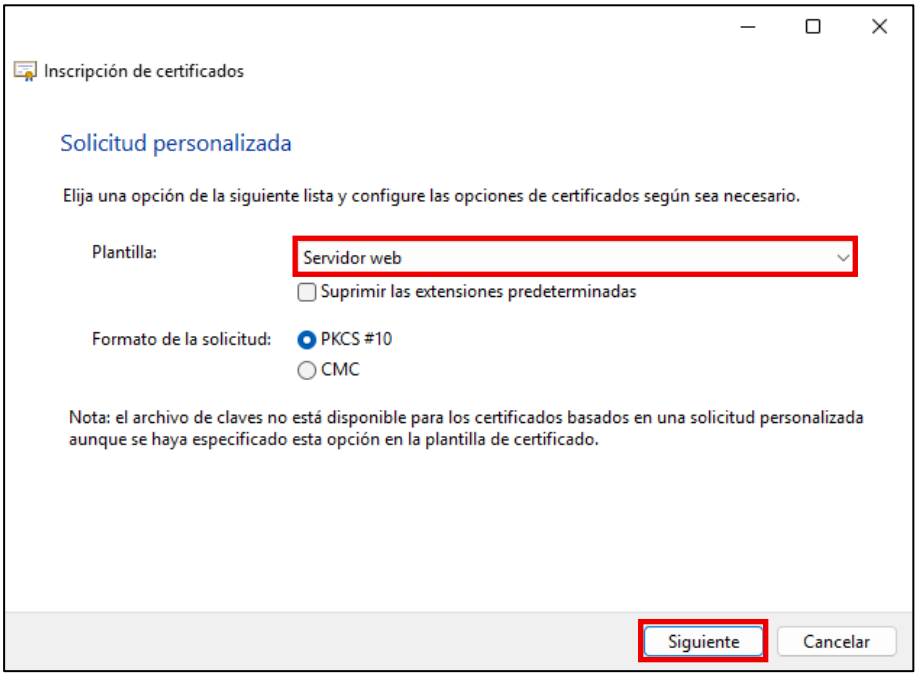


Ilustración 65 - Selección de la plantilla

20.	Despliegue “Servidor web” y haga clic en “Propiedades”.

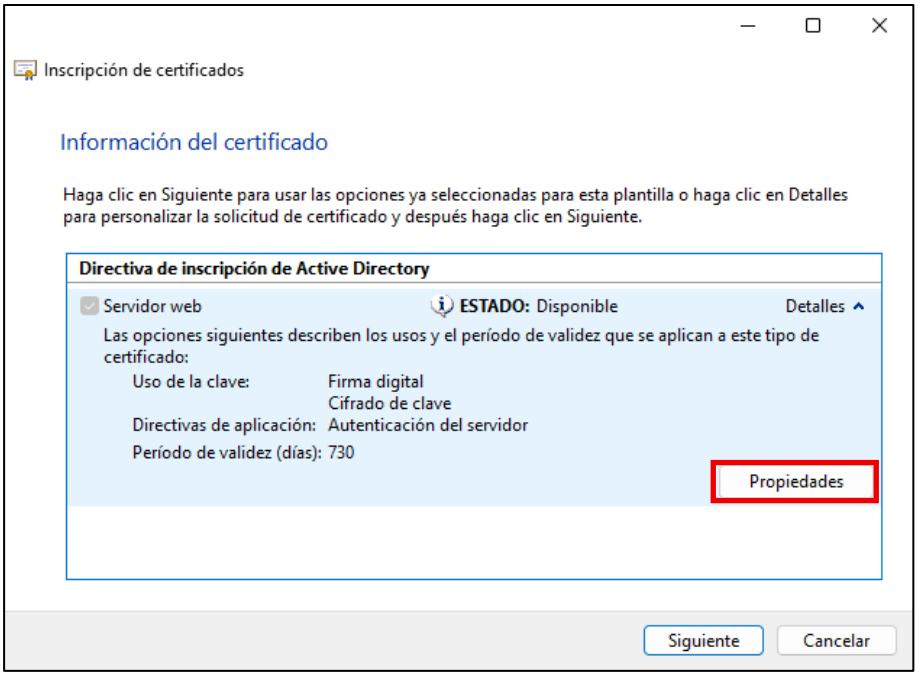


Ilustración 66 - Propiedades de la solicitud

21.	En la pestaña “Sujeto”, indique el nombre de sujeto, y, en el apartado “Nombre alternativo”, desplegar la lista y seleccionar “DNS”. Agregar los siguientes valores:

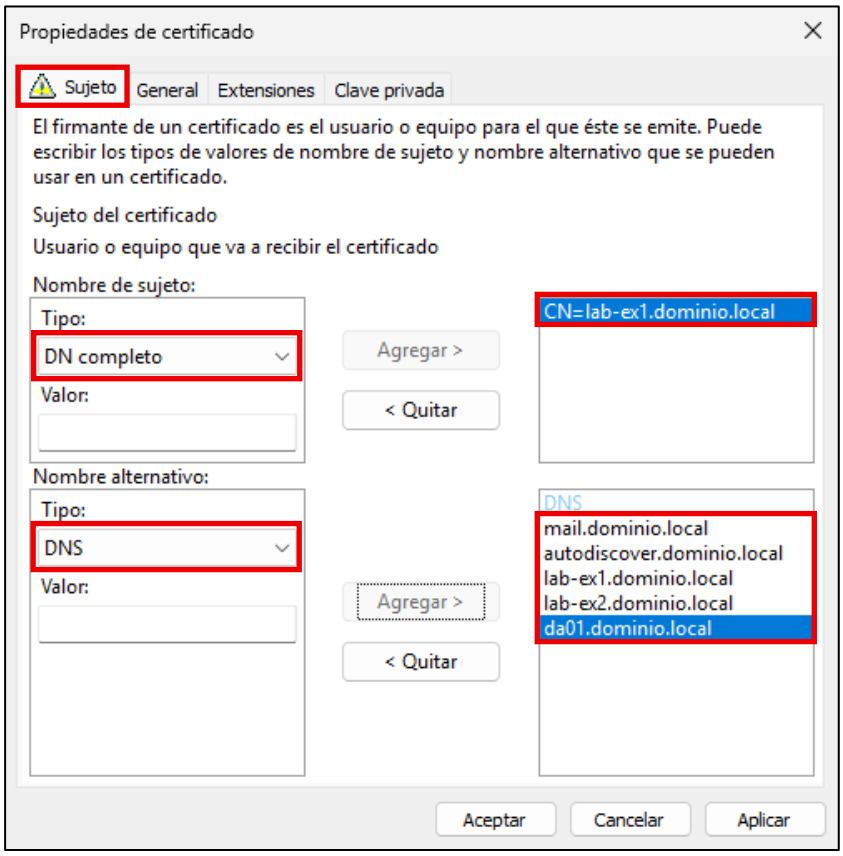
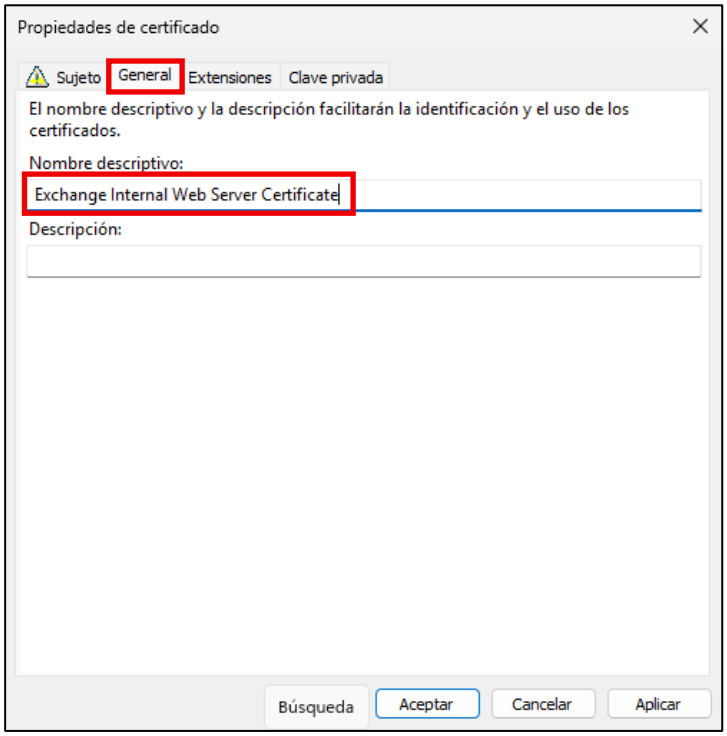
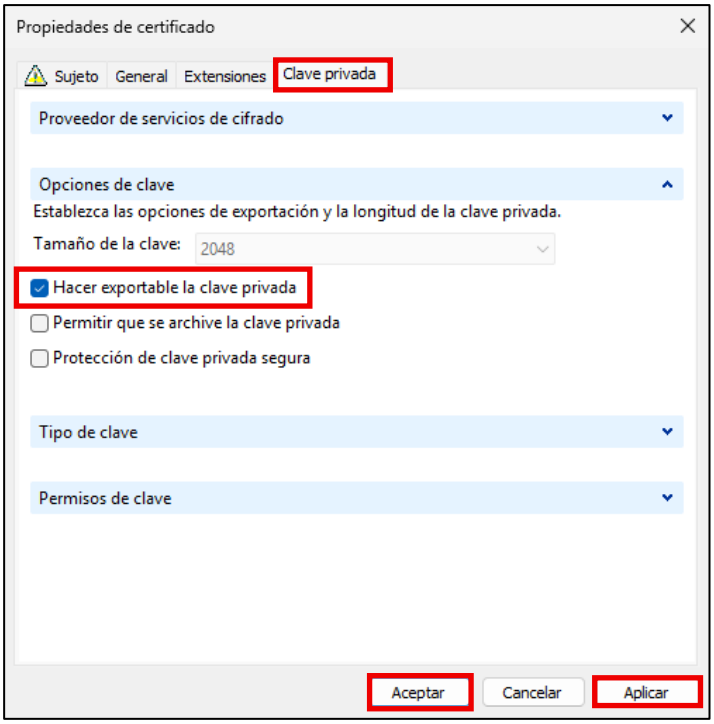


Ilustración 67 - Configuración del sujeto

Nota: como se puede observar, se ha agregado el nombre de equipo utilizado para la configuración del DAG en Exchange.

22.	En la pestaña “General”, indique un nombre descriptivo para el mismo.  *Ilustración 68 - Configuración general*
23.	En la pestaña “Clave privada”, despliegue “Opciones de clave” y marque la casilla “Hacer exportable la clave privada”. Haga clic en “Aplicar” y “Aceptar”.  *Ilustración 69 - Configuración de la clave privada*

24.	En la ventana de solicitud de certificado, marque ahora “Servidor web” y haga clic en “Siguiente”.

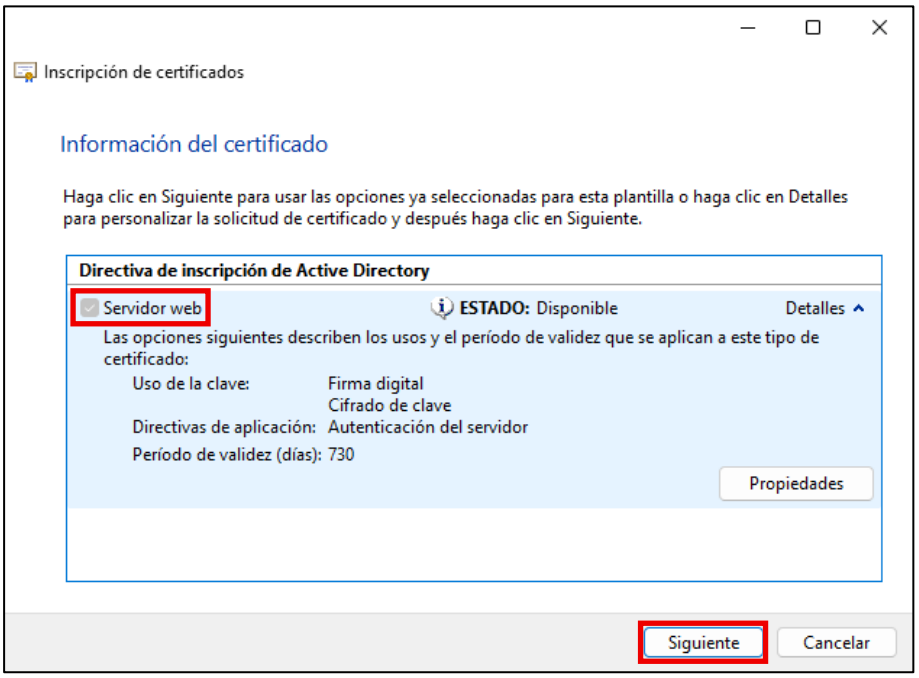


Ilustración 70 - Configuración de la solicitud

25.	Seleccione una ruta y nombre de archivo para la exportación y haga clic en “Finalizar”.

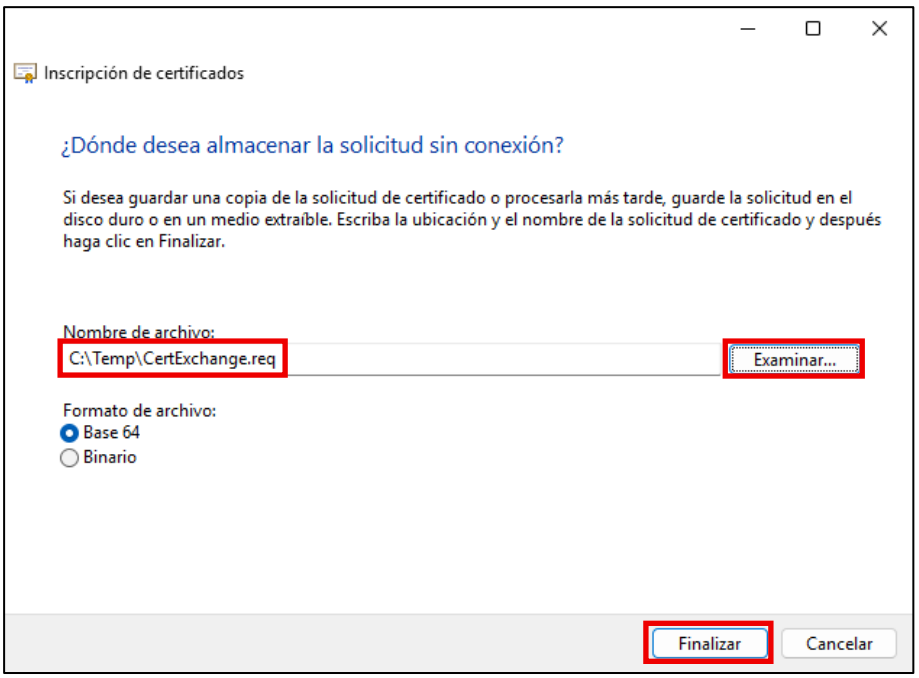
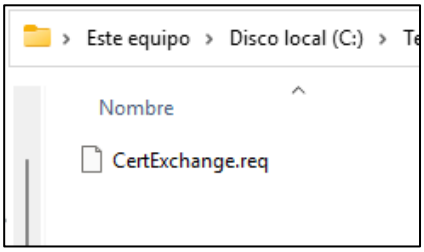
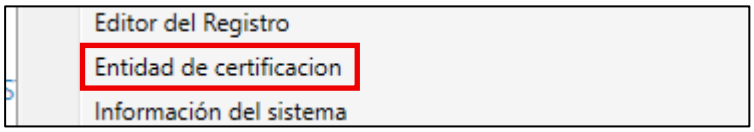
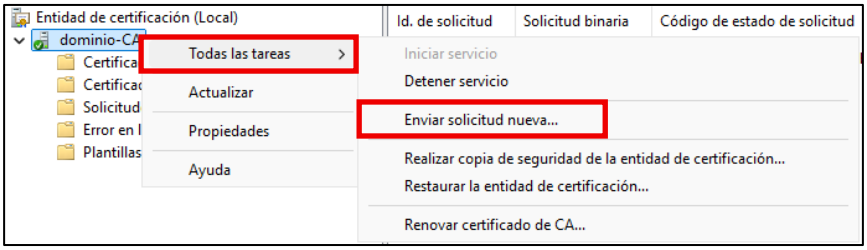
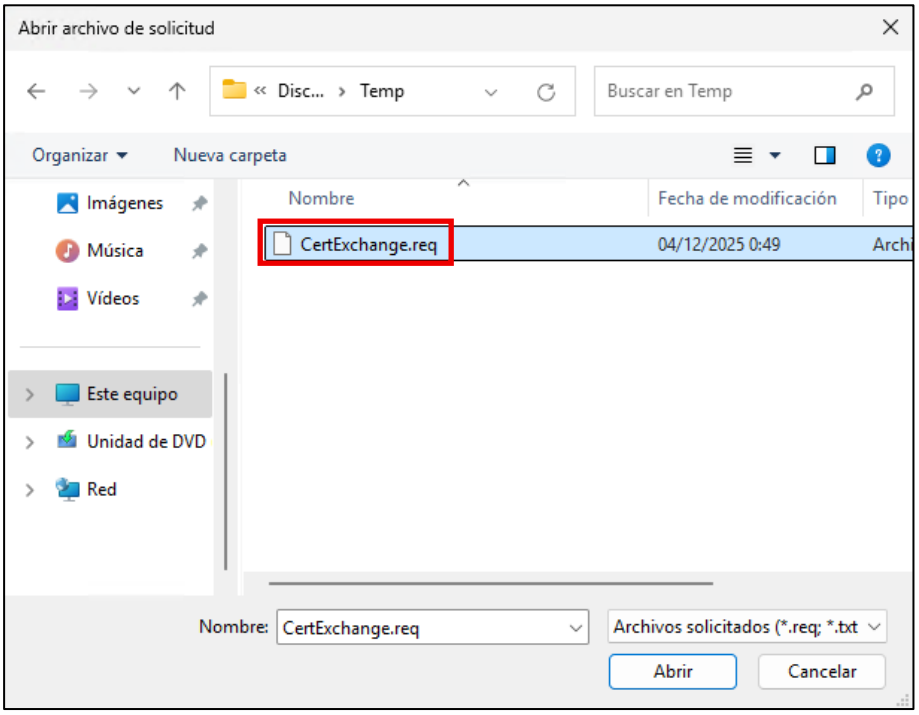
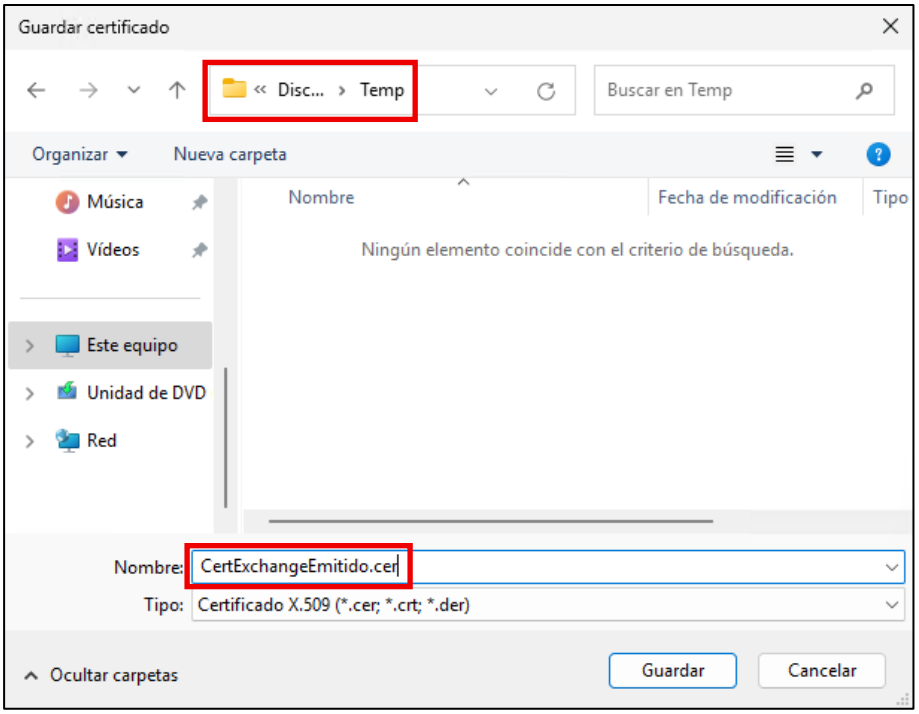


Ilustración 71 - Exportación del archivo

26.	Copie el archivo al servidor Entidad de certificación.  *Ilustración 72 - Copia del archivo*
27.	Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en el servidor Entidad de Certificación.
28.	En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Entidad de certificación”.  *Ilustración 73 - Entidad de certificación*
29.	Haga clic derecho sobre la entidad de certificación y seleccione “Todas las tareas > Enviar solicitud nueva”.  *Ilustración 74 - Envío de solicitud nueva*

30.	Seleccione la solicitud recién copiada.  *Ilustración 75 - Selección del archivo*
31.	Seleccione ruta y nombre para el certificado emitido.  *Ilustración 76 - Exportación del certificado*

32.	Copie el certificado recién emitido al servidor de Exchange.

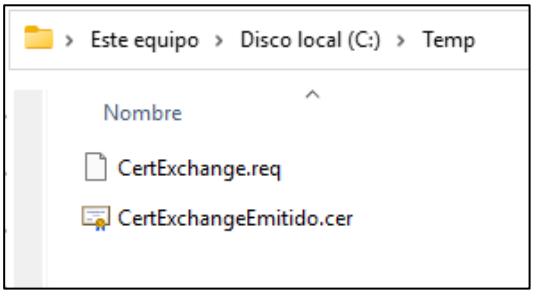


Ilustración 77 - Copia del archivo

33.	Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en uno de los servidores que alojan el servicio Exchange Server SE.
34.	Sobre la barra de búsqueda, escriba “Exchange Management Shell”.

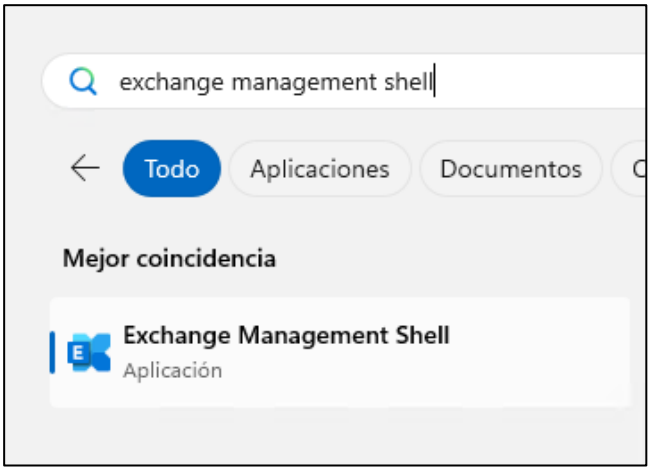


Ilustración 78 - Exchange Management Shell

35.	Haga clic derecho y seleccione “Ejecutar como administrador”.

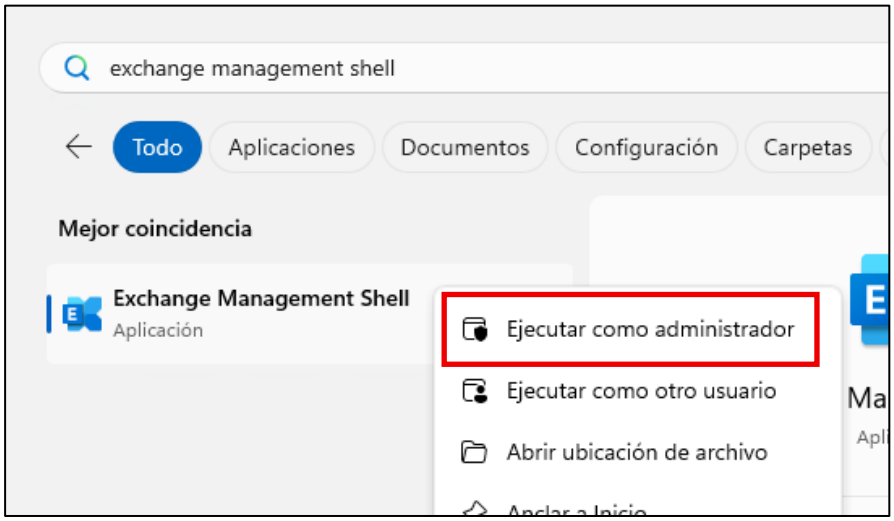
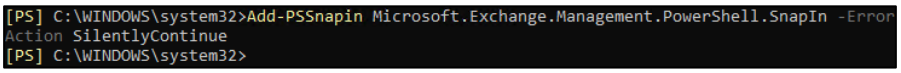
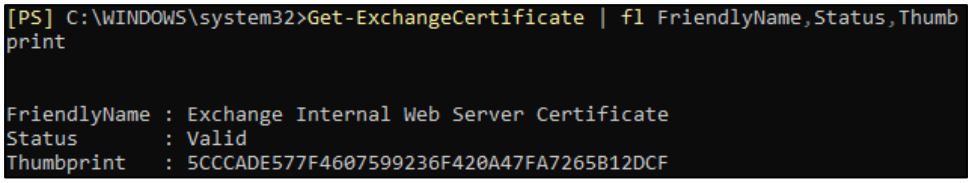
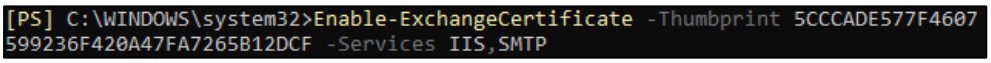
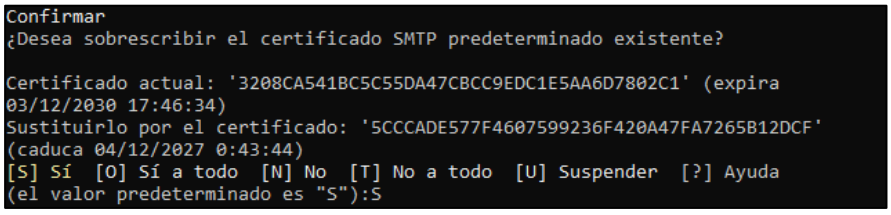


Ilustración 79 - Ejecución como administrador

36.	Introduzca el siguiente comando para habilitar todas las opciones.
	> Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn -ErrorAction SilentlyContinue.
	 *Ilustración 80 - Adición de SnapIn*
37.	Introduzca el siguiente comando para importar el certificado emitido a Exchange.
	> $certPath = “C:\Temp\CertExchangeEmitido.cer” > $cert = Import-ExchangeCertificate -FileData ([Byte[]]$(Get-Content -Path $certPath -Encoding byte -ReadCount 0))
	 *Ilustración 81 - Importación del certificado*
38.	Introduzca el siguiente comando para anotar el “Thumbprint” del certificado.
	 *Ilustración 82 - Copia del "Thumbprint"*
39.	Introduzca el siguiente comando para configurar dicho certificado para los servicios necesarios.
	 *Ilustración 83 - Habilitación del certificado*
40.	Escriba “S” y pulse “Enter”.
	 *Ilustración 84 - Confirmación de sustitución*
41.	Repita los pasos 37 al 40 incluidos en el servidor secundario de Exchange.
42.	Reinicie los servidores de Exchange.

ANEXO A.2.2. Asignación de Permisos y Roles

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

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

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

Paso	Descripción
1.	Inicie sesión con un usuario miembro del grupo Admins. de Dominio en un equipo o servidor miembro del dominio.
2.	Ejecute Microsoft Edge y escriba “https://” seguido del FQDN de uno de los servidores de Exchange, y seguido de “/ecp”.  *Ilustración 85 - Acceso al centro de administración*
3.	Inicie sesión con el usuario con el que se configuró Exchange. Para ello, escriba primero el nombre de su dominio, “\”, y el nombre de usuario.  *Ilustración 86 - Inicio de sesión*

4.	En el panel izquierdo, haga clic en “permisos”. En el panel derecho, haga clic en “roles de administrador”.

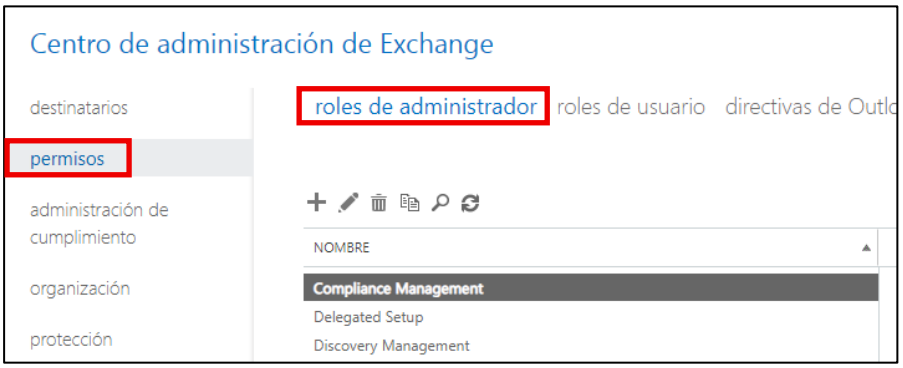


Ilustración 87 - Roles de administrador

5.	Desde este menú, puede asignar roles de administrador predeterminados a grupos nuevos o existentes en la organización, así como crear nuevos roles con permisos específicos.
6.	Por ejemplo, **“Discovery Management”** Tiene asignados los permisos necesarios para trabajar con la retención legal, así como la suspensión y exhibición de datos electrónicos. Sus permisos incluyen la realización de búsquedas de buzones en la organización para obtener datos que cumplan determinados criterios, así como la configuración de retenciones legales en los diferentes buzones de correo.

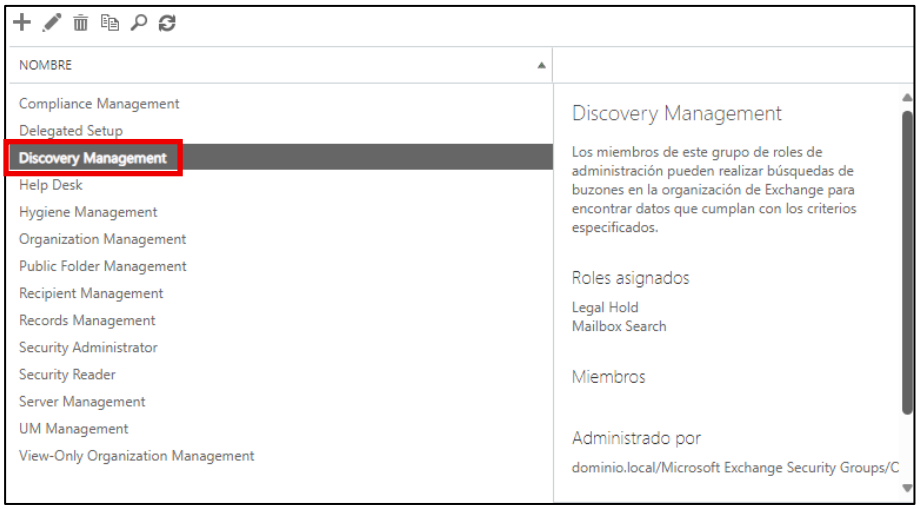
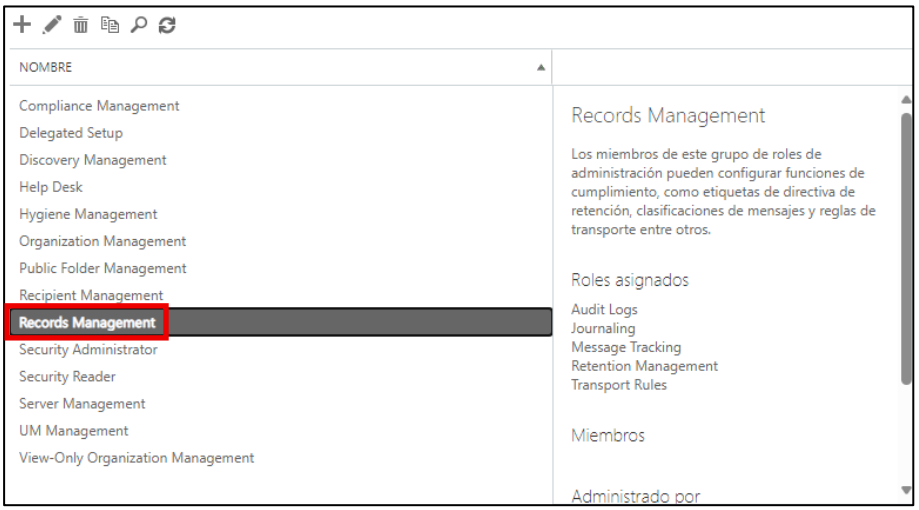
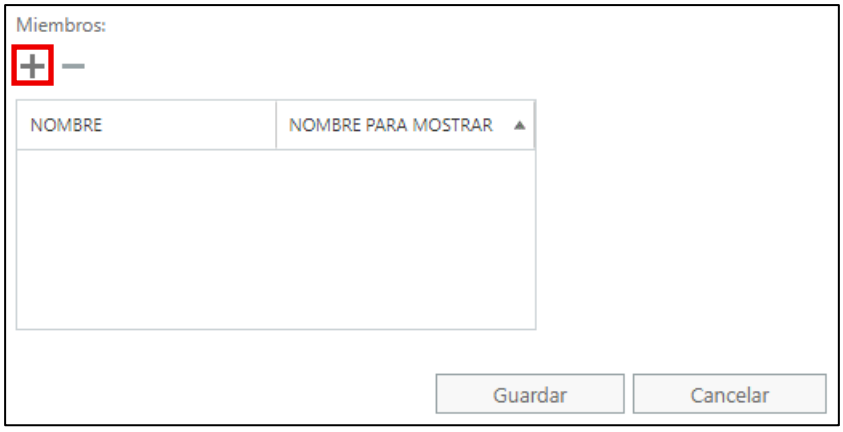


Ilustración 88 - Discovery Management

7.	**"Records Management"** tiene permisos relativos a las capacidades de auditoría. A continuación, se explica cómo asignar dicho rol a un grupo de seguridad del Directorio Activo. Para ello, haga clic sobre el icono del lápiz.  *Ilustración 89 - Records Management*
8.	Pulse sobre el símbolo "+" en "Miembros".  *Ilustración 90 - Adición de miembros*
9.	Seleccione el grupo deseado (a modo de ejemplo, se seleccionará "Help Desk"). Después, haga clic en "Agregar" y en "Aceptar".

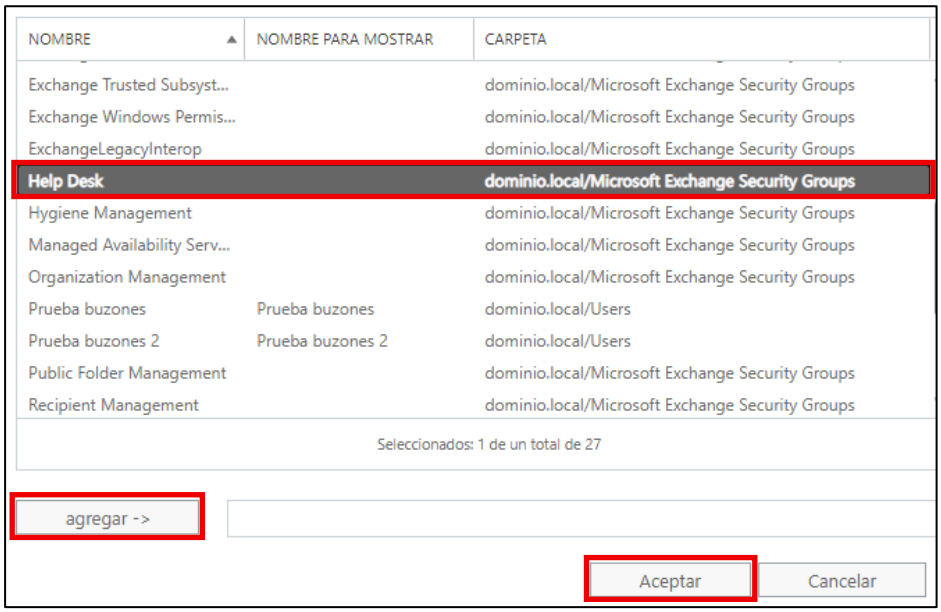


Ilustración 91 - Selección de miembros

10. Haga clic en “Guardar” para que los cambios se hagan efectivos.

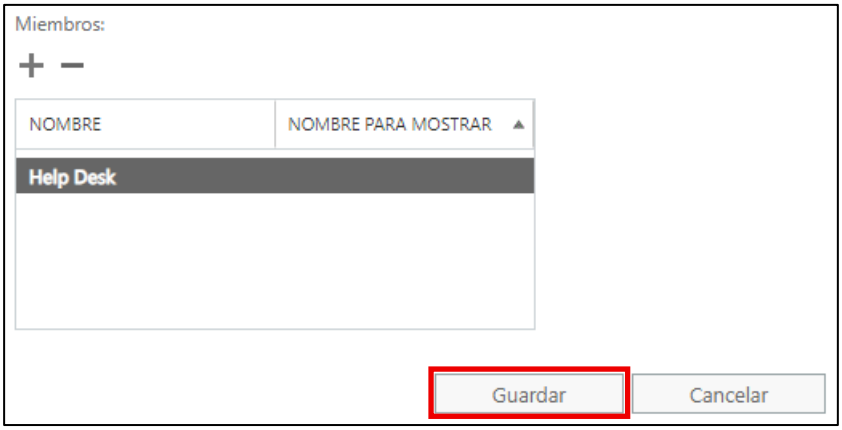
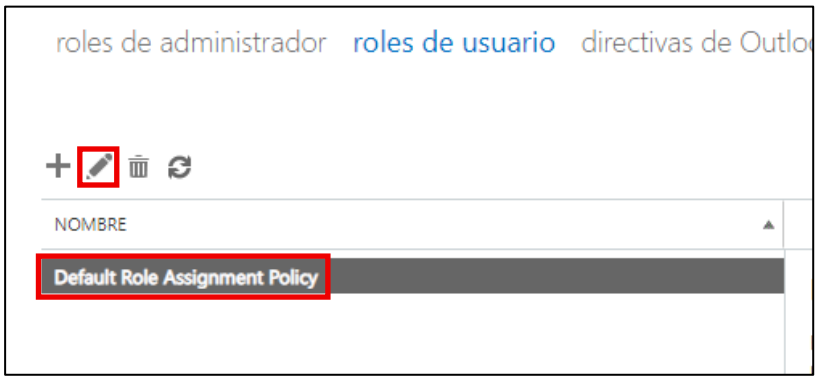
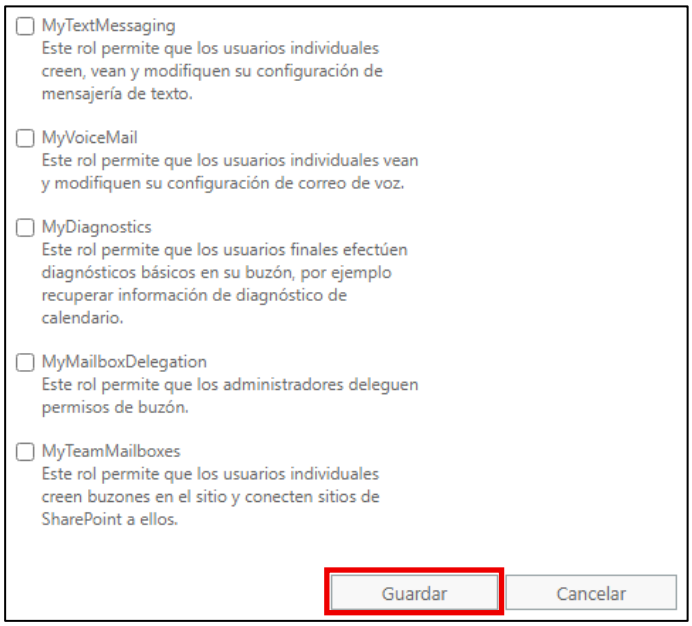
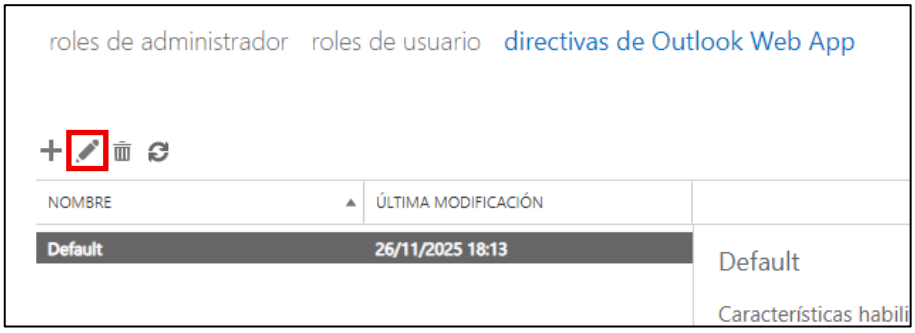
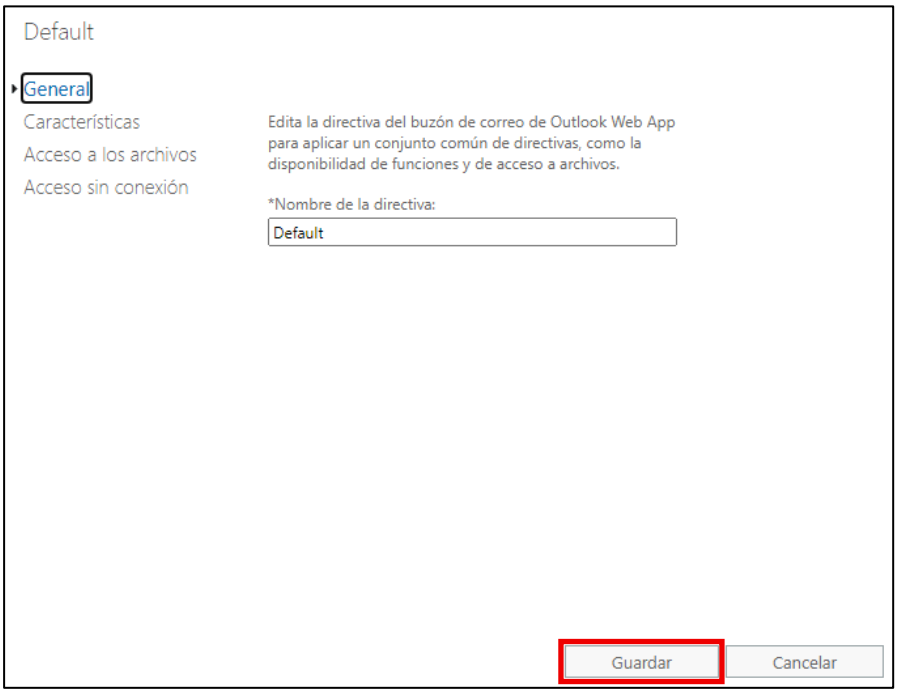
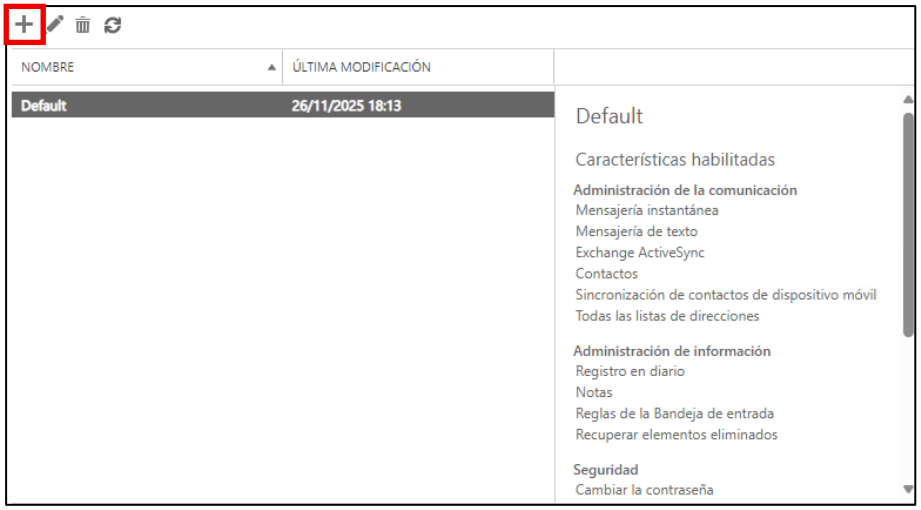
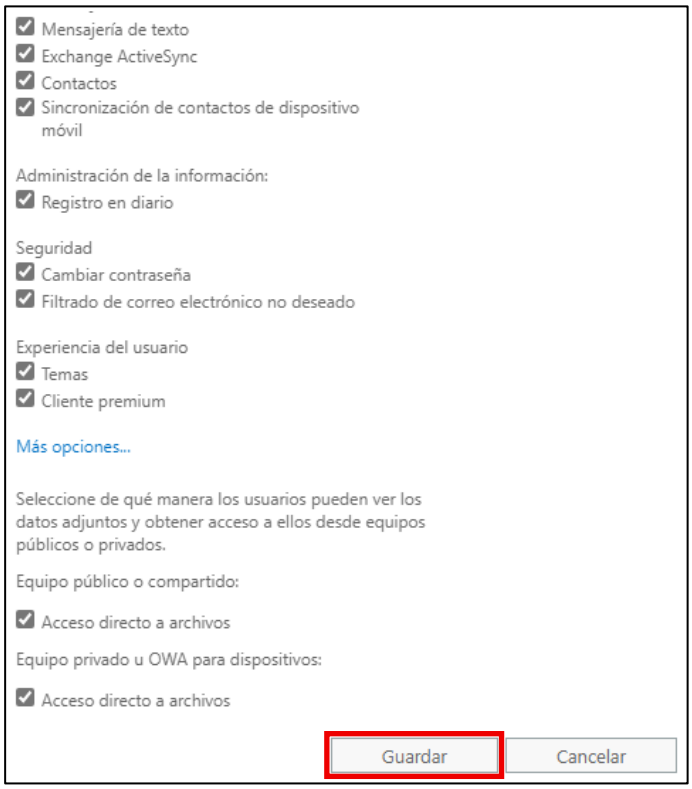


Ilustración 92 - Guardado de la configuración

11.	Puede también cambiar el grupo de roles de usuario por defecto. Para ello, haga diríjase a “roles de usuario” en el panel derecho, y, seleccionando el grupo “Default Role Assignment Policy”, haga clic sobre el icono del lápiz. Dentro, puede modificar los campos que se precisen para adecuar la configuración a la de la organización.  *Ilustración 93 - Default Role Assignment Policy*
12.	De igual manera, es posible crear un grupo de roles de usuario nuevo. Para ello, seleccione la pestaña “roles de usuario” y haga clic sobre “+”.  *Ilustración 94 – Creación de grupos de roles*

13.	Marque los campos correspondientes en función de las necesidades de su organización y pulse “Guardar”.  *Ilustración 95 - Guardado de la configuración*
14.	Puede también cambiar las directivas de Outlook Web App (OWA). Para ello, diríjase a la pestaña “directivas de Outlook Web App”, seleccione la opción “Default” y haga clic sobre el icono del lápiz.  *Ilustración 96 - Edición de "Default"* **Nota:** el valor “Default” de directiva de Outlook Web App tiene todas las opciones habilitadas de forma predeterminada.

15.	Configure los campos correspondientes en función de las necesidades de la organización y pulse “Guardar”.  *Ilustración 97 - Guardado de la configuración*
16.	Si precisa de crear un grupo de directivas nuevo, haga clic sobre “+”.  *Ilustración 98 - Creación de grupo de directivas*

17.	Rellene los campos que precise necesarios para la organización y haga clic en “Guardar”.  *Ilustración 99 - Guardado de la configuración*

ANEXO A.2.3. Configuración de Registro de Actividad

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

Mediante el registro de auditoría de buzón, es posible 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.

Paso	Descripción
1.	Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en uno de los servidores que alojan el servicio Exchange Server SE.

2.	Sobre la barra de búsqueda, escriba “Exchange Management Shell”.

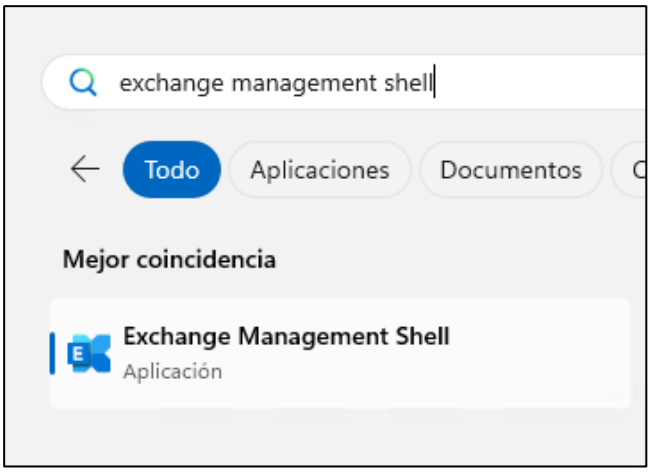


Ilustración 100 - Exchange Management Shell

3.	Haga clic derecho y seleccione “Ejecutar como administrador”.

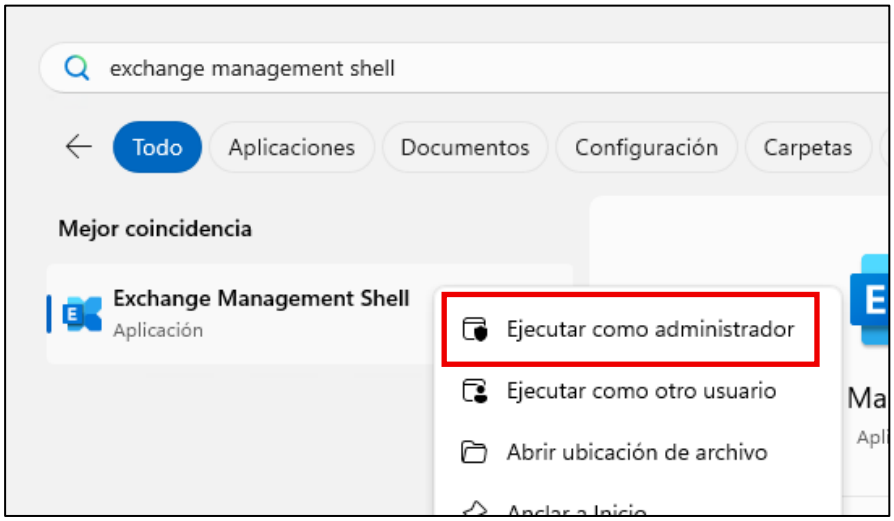


Ilustración 101 - Ejecución como administrador

4.	Introduzca el siguiente comando para habilitar todas las opciones.
	> Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn -ErrorAction SilentlyContinue.

```
[PS] C:\WINDOWS\system32>Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn -Error
Action SilentlyContinue
[PS] C:\WINDOWS\system32>
```

Ilustración 102 - Adición de SnapIn

5.	Ejecute el siguiente comando para habilitar las auditorías sobre un buzón. En este caso, se usará el buzón de uno de los usuarios de pruebas creados con anterioridad.
	> Set-Mailbox prueba.buzones1 -AuditEnable $true

> Get-Mailbox | fl Name,auditEnabled

```
[PS] C:\WINDOWS\system32>Set-Mailbox prueba.buzones1 -AuditEnable $true
[PS] C:\WINDOWS\system32>Get-Mailbox | fl Name,auditEnabled


Name          : da001
AuditEnabled : False

Name          : DiscoverySearchMailbox
                {D919BA05-46A6-415f-80AD-7E09334BB852}
AuditEnabled : False

Name          : Prueba buzones
AuditEnabled : True

Name          : Prueba buzones 2
AuditEnabled : False
```

Ilustración 103 - Habilitación de auditorías

6. Es posible exportar los registros de auditoría de buzones desde la consola Web de administración. Para ello, inicie sesión con un usuario miembro del grupo Admins. de Dominio en un equipo o servidor miembro del dominio.

7. Ejecute Microsoft Edge y escriba “https://” seguido del FQDN de uno de los servidores de Exchange, y seguido de “/ecp”.

Ilustración 104 - Acceso al centro de administración

8. Inicie sesión con el usuario con el que se configuró Exchange. Para ello, escriba primero el nombre de su dominio, “\”, y el nombre de usuario.

Ilustración 105 - Inicio de sesión

9.	En el panel izquierdo, seleccione “administración de cumplimiento”. En el panel derecho, diríjase a la pestaña “auditoría”, y haga clic sobre “Exportar registros de auditoría de buzones de correo”.

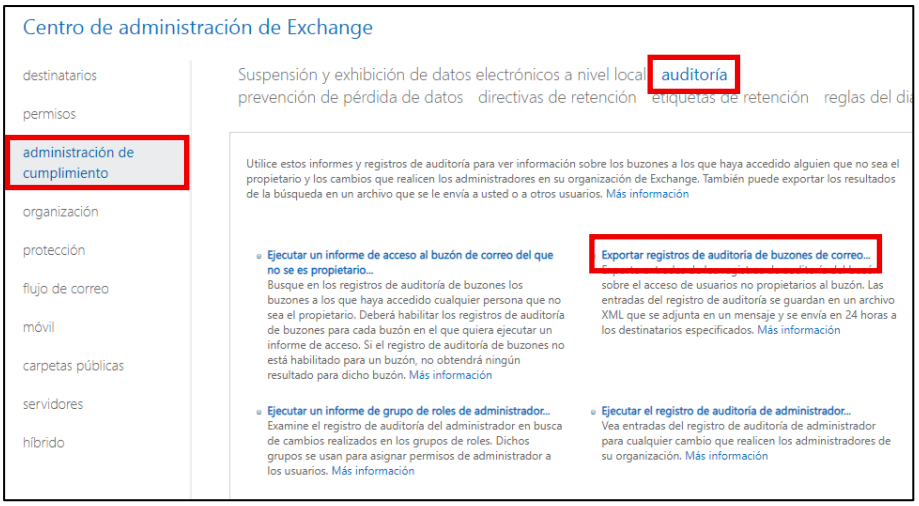


Ilustración 106 - Exportación de registros de auditoría

10.	Establezca el intervalo de fechas, los buzones donde desea buscar y el buzón de destino del informe. Una vez cumplimentada toda la información, haga clic en “exportar”.

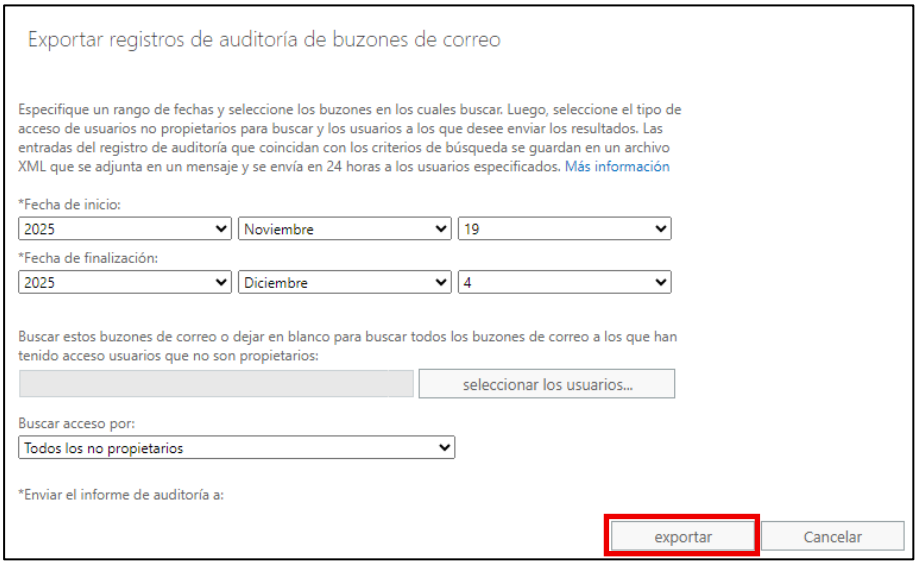
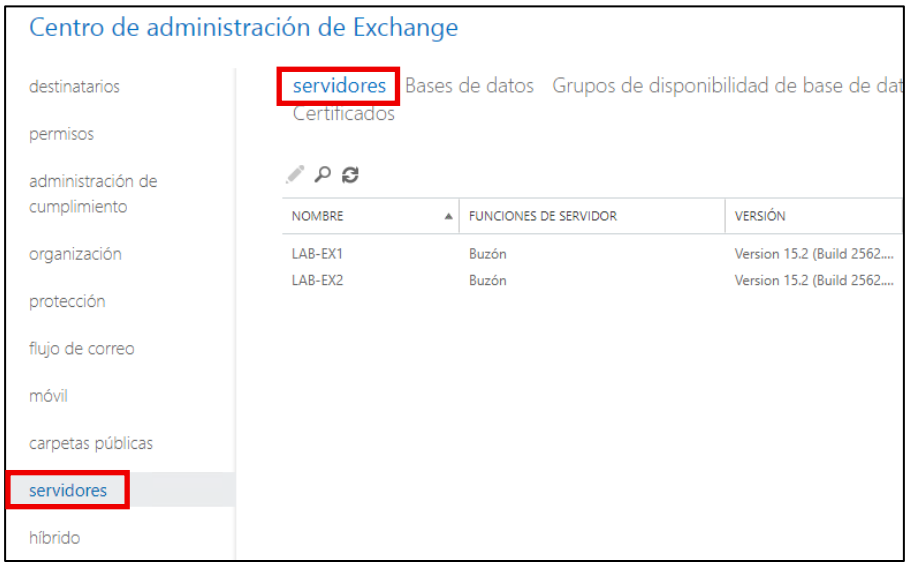
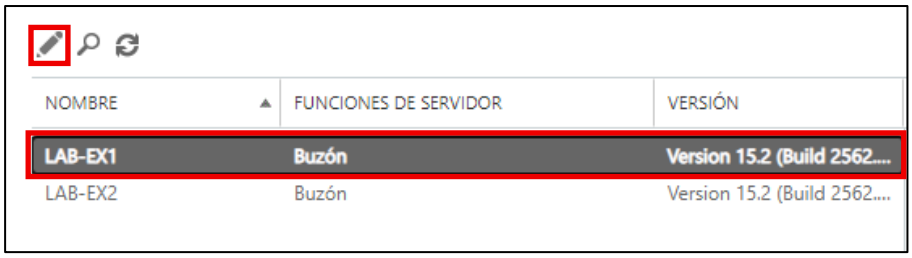


Ilustración 107 - Configuración del informe

Nota: Exchange puede llegar a tardar 24 horas en generar el informe y enviarlo

ANEXO A.2.4. Configuración de Registro de Seguimiento de Mensajes

Paso	Descripción
1.	Inicie sesión con un usuario miembro del grupo Admins. de Dominio en un equipo o servidor miembro del dominio.
2.	Ejecute Microsoft Edge y escriba “https://” seguido del FQDN de uno de los servidores de Exchange, y seguido de “/ecp”.  *Ilustración 108 - Acceso al centro de administración*
3.	Inicie sesión con el usuario con el que se configuró Exchange. Para ello, escriba primero el nombre de su dominio, “\”, y el nombre de usuario.  *Ilustración 109 - Inicio de sesión*

4.	En el panel izquierdo, seleccione “servidores”. En el panel derecho, diríjase a la pestaña “servidores”,  *Ilustración 110 - Servidores*
5.	Seleccione uno de los servidores de Exchange y haga clic en el icono del lápiz.  *Ilustración 111 - Edición de servidores*

6.	En la sección de “Registros de transporte”, puede modificar la configuración de almacenamiento de cada uno de los registros, habilitar y deshabilitar el “Registro de seguimiento de mensajes” y el “Registro de conectividad”. Haga clic en “Guardar”.

Ilustración 112 - Guardado de configuración

7.	Seleccione “flujo de correo” en el panel izquierdo, e “informes de entrega” en el panel derecho. Ahí podrá ejecutar el registro de seguimiento de mensajes.

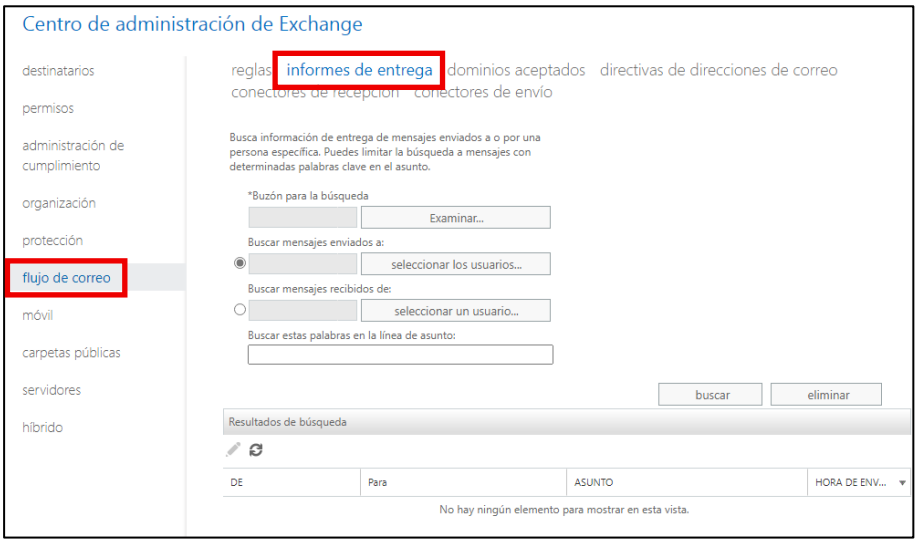
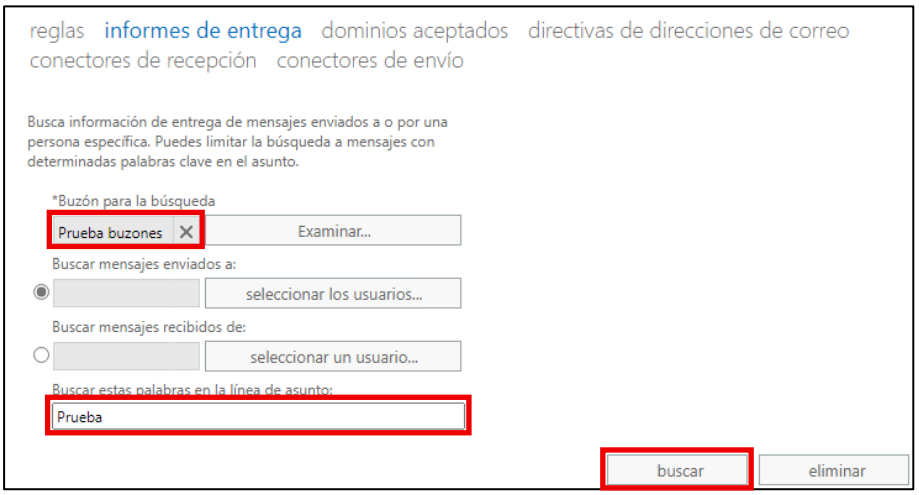
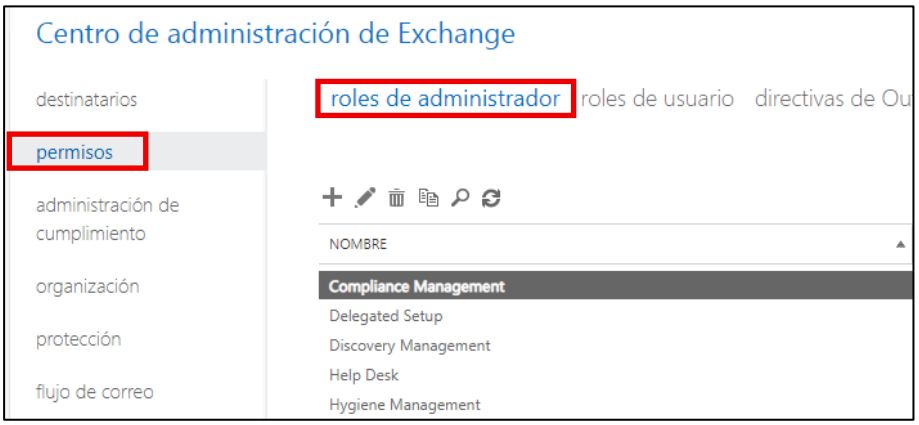
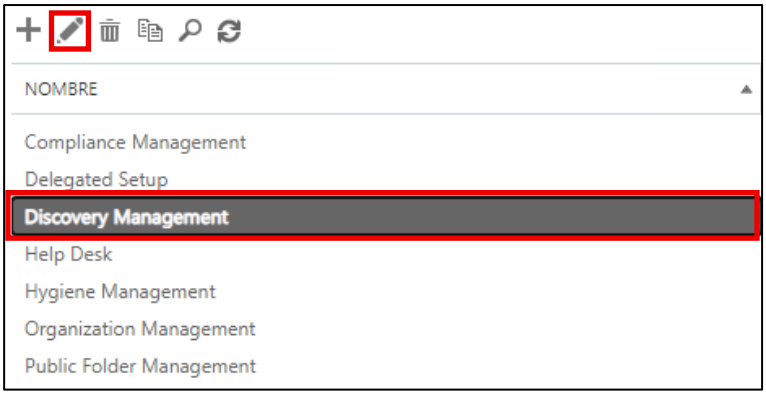


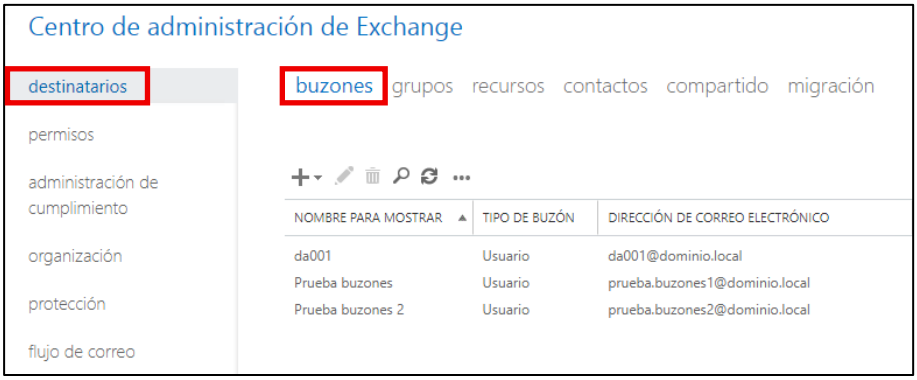
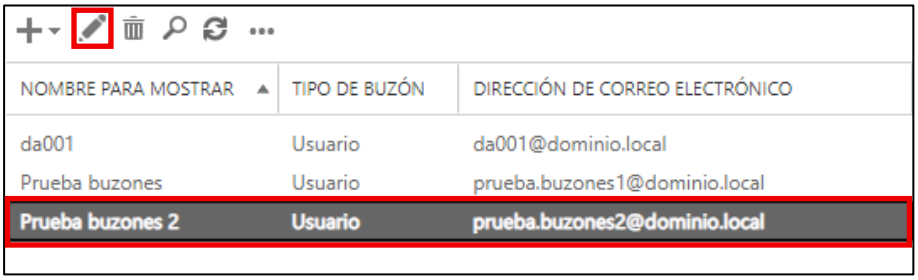
Ilustración 113 - Informes de entrega

8.	Puede seleccionar un buzón y hacer clic en “buscar” para comenzar la búsqueda.  *Ilustración 114 - Filtrado para búsqueda*
9.	Haciendo doble clic sobre los resultados, puede enviar al usuario afectado el informe.

ANEXO A.2.5. Configuración de Registro de la Gestión de Incidentes

Paso	Descripción
1.	Inicie sesión con un usuario miembro del grupo Admins. de Dominio en un equipo o servidor miembro del dominio.
2.	Ejecute Microsoft Edge y escriba “https://” seguido del FQDN de uno de los servidores de Exchange, y seguido de “/ecp”.  *Ilustración 115 - Acceso al centro de administración*
3.	Inicie sesión con el usuario con el que se configuró Exchange. Para ello, escriba primero el nombre de su dominio, “\”, y el nombre de usuario.  *Ilustración 116 - Inicio de sesión*

4.	En el panel izquierdo, haga clic en “permisos”, y seleccione la pestaña “roles de administrador”.  *Ilustración 117 - Roles de administrador*
5.	Seleccione el grupo de roles “Discovery Management” y haga clic sobre el icono del lápiz.  *Ilustración 118 - Edición de "Discovery Management"*

6.	En la sección “Miembros”, haga clic sobre “+” y agregue las cuentas de los usuarios a los que desee aplicarles este grupo de roles. Haga clic en “Guardar” cuando haya finalizado.  *Ilustración 119 - Adición de miembros* **Nota:** a modo de ejemplo, se utiliza el usuario “da001”. Se deberá agregar el usuario/grupo de usuarios que se considere necesario.
7.	Habilite la retención por juicio en un buzón de usuario. Para ello, en el panel izquierdo haga clic en “destinatarios”, y en el panel derecho diríjase a la pestaña “buzones”.  *Ilustración 120 - Habilitación de retención por juicio*
8.	Seleccione el buzón en el cual desea habilitar retención por juicio y haga clic en el icono del lápiz.  *Ilustración 121 - Edición del buzón*

9.	Haga clic en “Características de buzón” y habilite “Retención por juicio”.

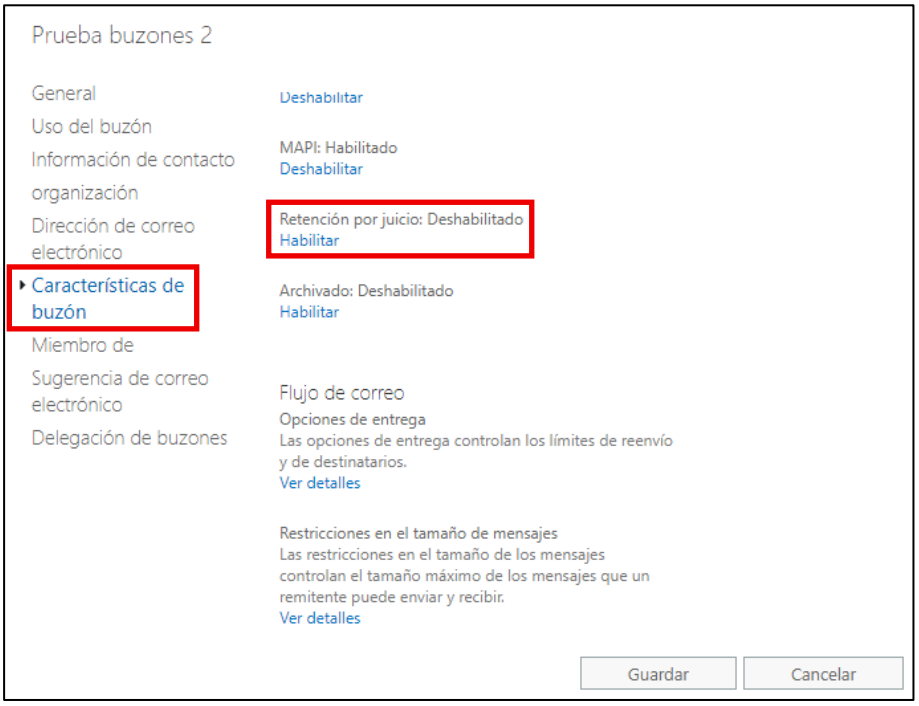


Ilustración 122 - Habilitación de la configuración

10.	Establezca el período necesario y haga clic en “Guardar”.

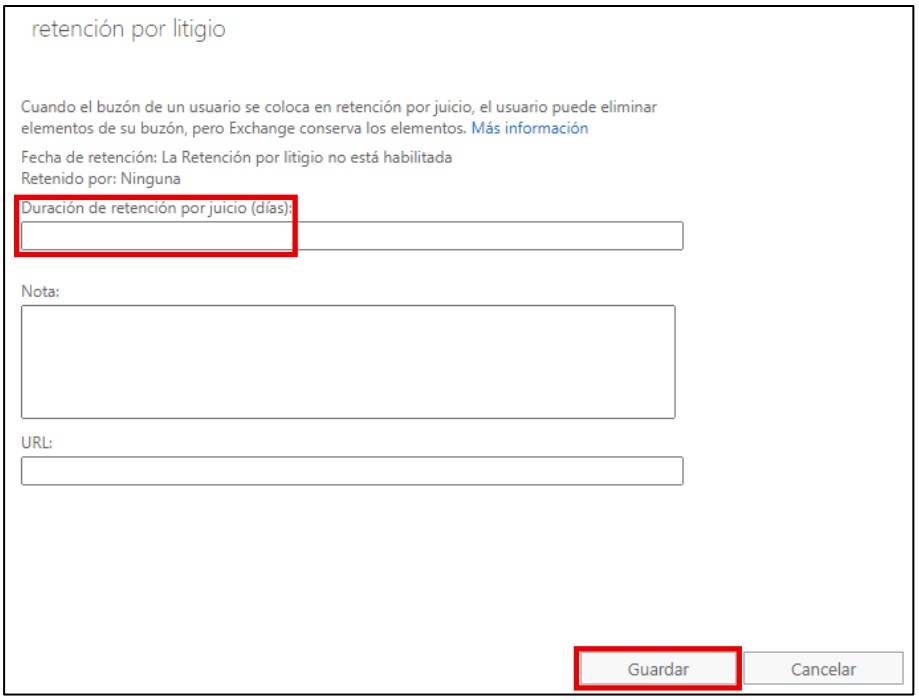


Ilustración 123 - Duración de la retención

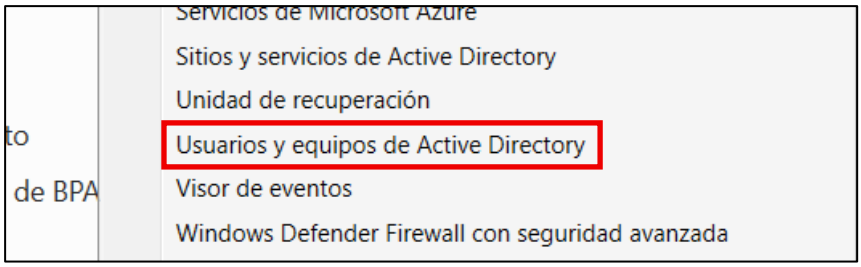
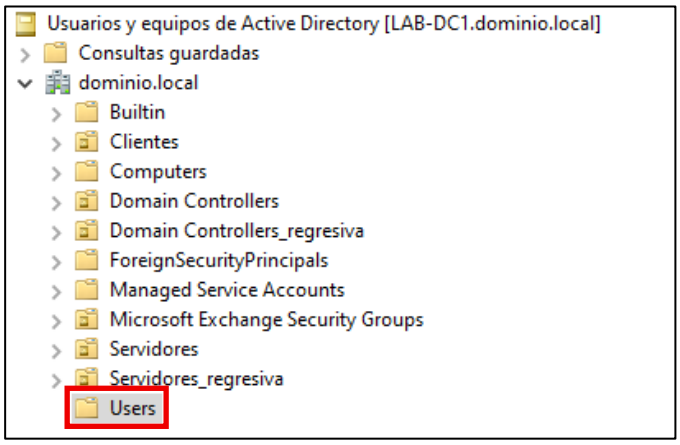
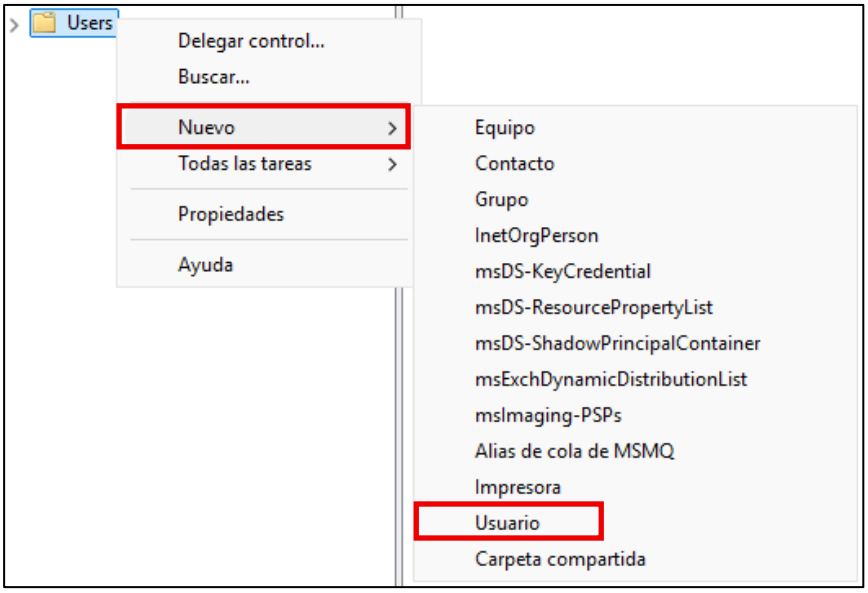
11.	Por último, para obtener un informe sobre los elementos que han sido modificados o eliminados en un buzón con retención legal habilitada, siga las siguientes instrucciones. En el panel izquierdo, haga clic en “administración de cumplimiento”. En el panel derecho, sitúese en la pestaña “auditoría”. Haga clic en “Ejecutar un informe de retención por juicio sobre buzón”.

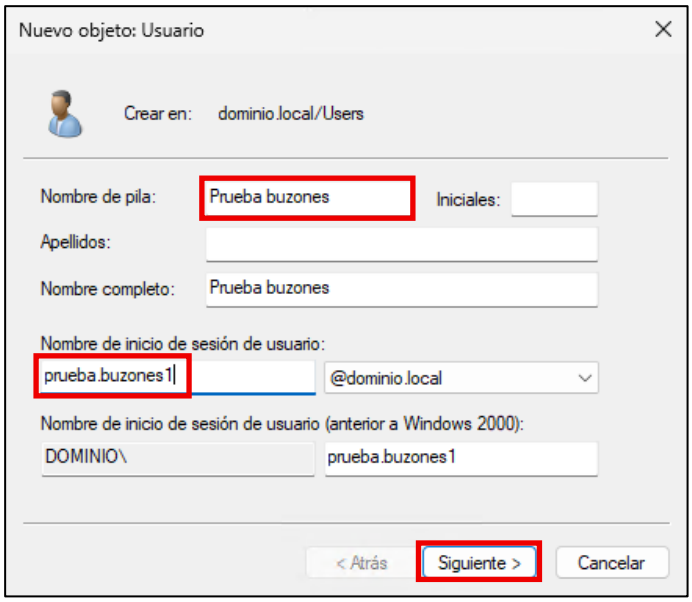
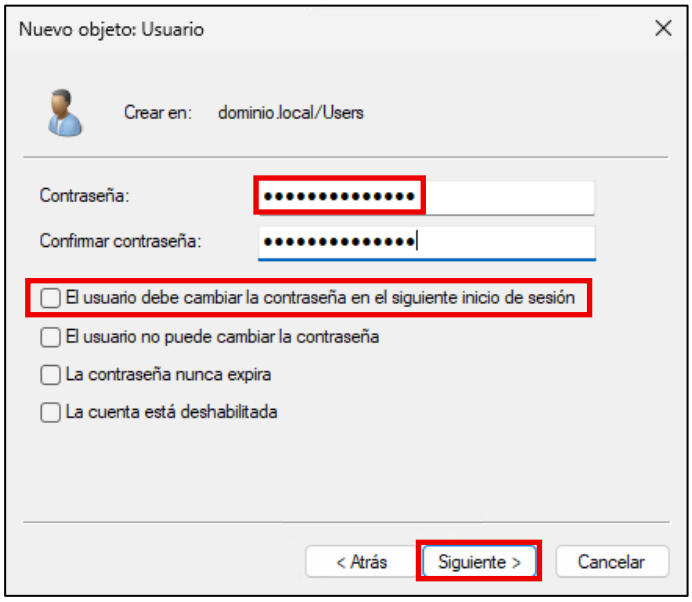
Ilustración 124 - Ejecución del informe de retención por juicio

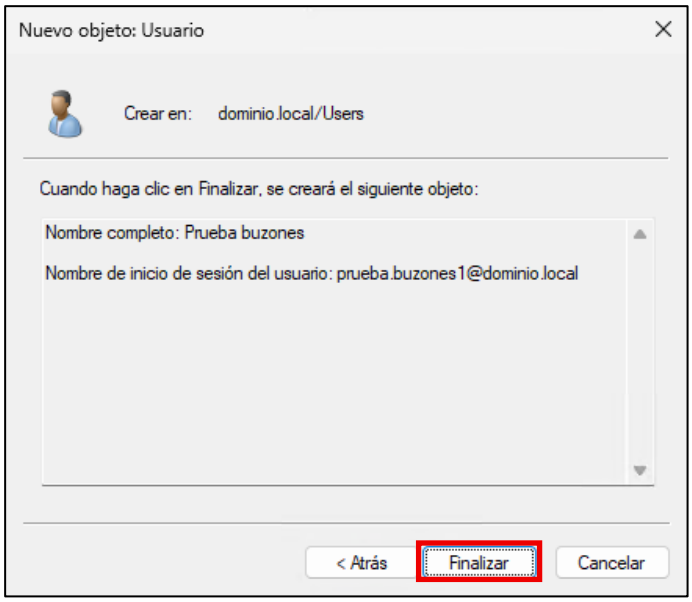
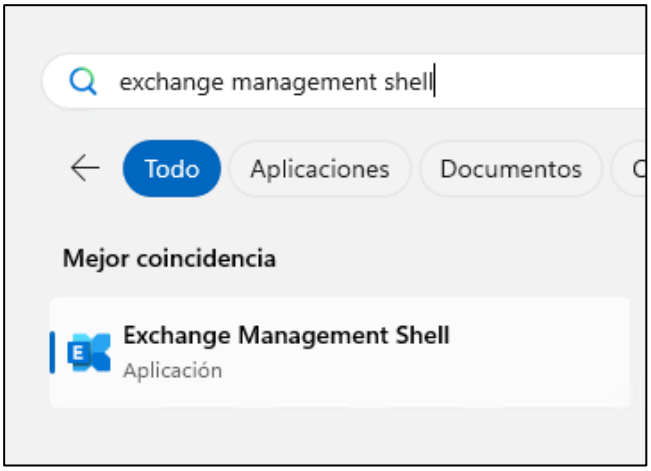
ANEXO A.3. Comprobaciones

En el presente anexo se lleva a cabo una prueba de comunicación que permite realizar una comprobación de conectividad fundamental, pues representa el tráfico de correo de un buzón a otro a través de la red de dominio. El envío del correo se puede realizar mediante interfaz en OWA, o mediante cmdlets de PowerShell. En esta ocasión, se ha realizado mediante PowerShell.

Paso	Descripción
12.	Inicie sesión con un usuario miembro del grupo Admins. de Dominio en un Controlador de Dominio.

13.	De nuevo en el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior, y seleccione “Usuarios y equipos de Active Directory”.  *Ilustración 125 - Usuarios y equipos de Active Directory*
14.	Despliegue la lista del panel izquierdo hasta visualizar el contenedor “Users”.  *Ilustración 126 - Users*
15.	Haga clic derecho sobre “Users” y seleccione la opción “Nuevo” > “Usuario”.  *Ilustración 127 - Creación de usuario*

16.	Introduzca los datos apropiados para un usuario de pruebas.  *Ilustración 128 - Datos del usuario*
17.	Establezca una contraseña y desmarque la casilla “El usuario debe cambiar la contraseña en el siguiente inicio de sesión”.  *Ilustración 129 - Contraseña del usuario*

18.	Haga clic en “Finalizar”.  *Ilustración 130 - Confirmación de creación*
19.	Repita la misma operación para crear otro usuario.
20.	Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en uno de los servidores que alojan el servicio Exchange Server SE.
21.	Sobre la barra de búsqueda, escriba “Exchange Management Shell”.  *Ilustración 131 - Exchange Management Shell*

22.	Haga clic derecho y seleccione “Ejecutar como administrador”.

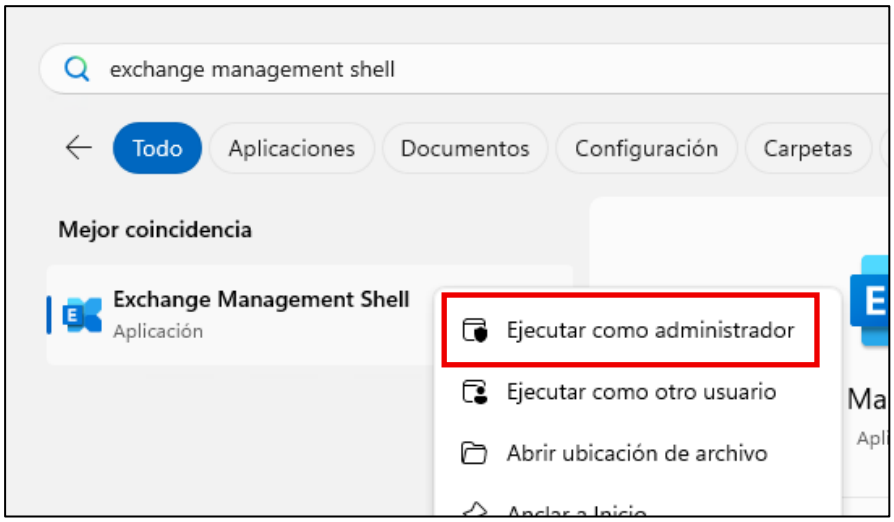


Ilustración 132 - Ejecución como administrador

23.	Introduzca el siguiente comando para habilitar todas las opciones.
	> Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn -ErrorAction SilentlyContinue

```
[PS] C:\WINDOWS\system32>Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn -Error
Action SilentlyContinue
[PS] C:\WINDOWS\system32>
```

Ilustración 133 - Adición de SnapIn

24.	Ejecute el siguiente comando para crear los buzones de los usuarios de prueba.

```
[PS] C:\WINDOWS\system32>Enable-Mailbox -Identity "prueba.buzones1" -Database "DB01"

Name                  Alias               ServerName      ProhibitSendQuota
----                  -----               ----------      -----------------
Prueba buzones        prueba.buzones1     lab-ex1         Unlimited


[PS] C:\WINDOWS\system32>Enable-Mailbox -Identity "prueba.buzones2" -Database "DB01"

Name                  Alias               ServerName      ProhibitSendQuota
----                  -----               ----------      -----------------
Prueba buzones 2      prueba.buzones2     lab-ex1         Unlimited
```

Ilustración 134 - Creación de buzones

25.	Inicie sesión con un usuario miembro del grupo Admins. de Dominio en un equipo o servidor miembro del dominio.

26.	Sobre la barra de búsqueda, escriba “PowerShell”.

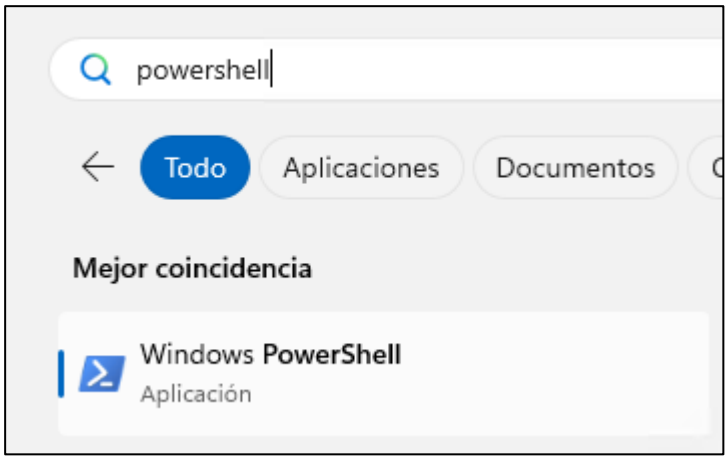


Ilustración 135 - Windows PowerShell

27.	Haga clic derecho, y seleccione “Ejecutar como administrador”

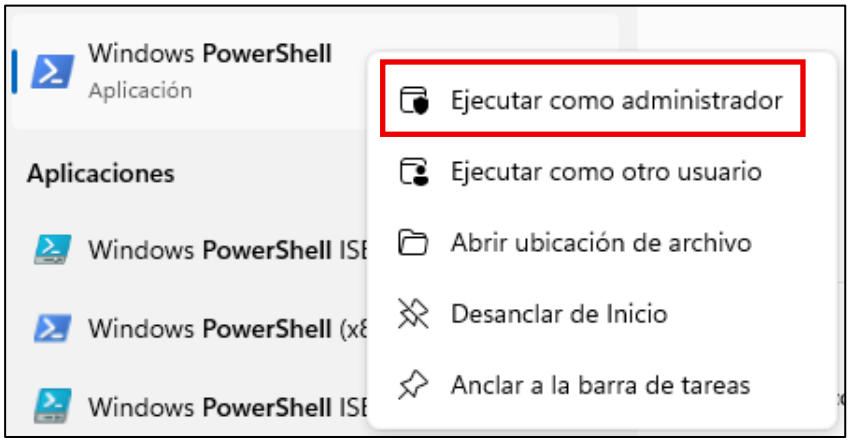


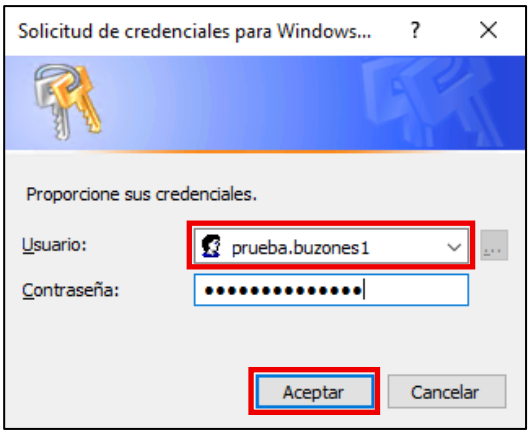
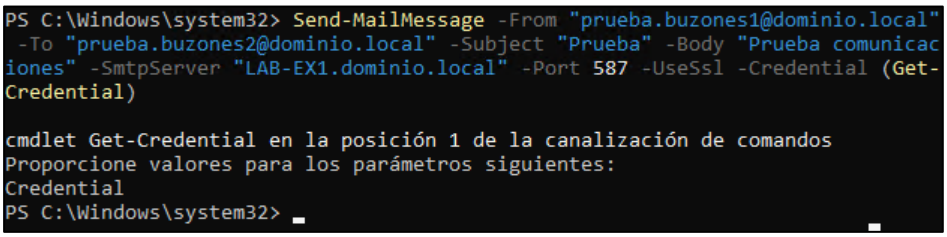
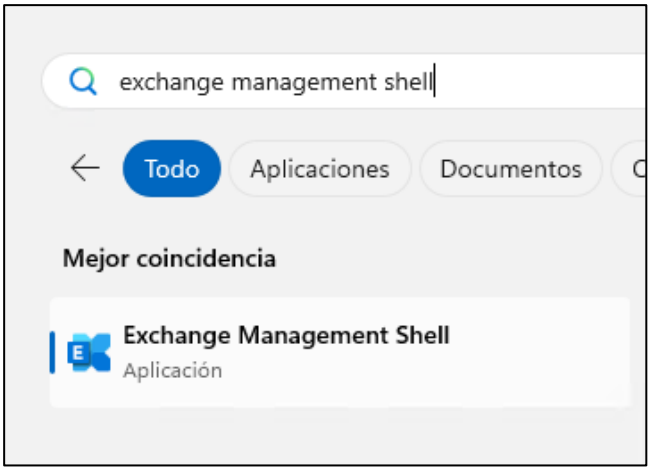
Ilustración 136 - Ejecución como administrador

28.	Introduzca el siguiente comando para enviar una comunicación hacia el buzón del otro usuario de pruebas.

> Send-MailMessage -From prueba.buzones1@dominio.local -To prueba.buzones2@dominio.local -Subject “Prueba” -Body “Esto es una prueba” -SmtpServer “lab-ex1.dominio.local” -Port 587 -UseSsl -Credential (Get-Credential)

Nota: Se debe tener en cuenta esto para rellenar los campos:

- “SmtpServer”: Se debe introducir el hostname del servidor de Exchange
- “From”: Se debe introducir el buzón del usuario que envía el correo
- “To”: Se debe introducir el buzón del usuario que recibe el correo

29.	En la ventana emergente, introduzca las credenciales de uno de los usuarios de pruebas.  *Ilustración 137 - Solicitud de credenciales*
30.	Asegúrese de que no recibe ningún error tras la ejecución del comando.  *Ilustración 138 - Envío del correo*
31.	Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en uno de los servidores que alojan el servicio Exchange Server SE.
32.	Sobre la barra de búsqueda, escriba “Exchange Management Shell”.  *Ilustración 139 - Exchange Management Shell*

33.	Haga clic derecho y seleccione “Ejecutar como administrador”.

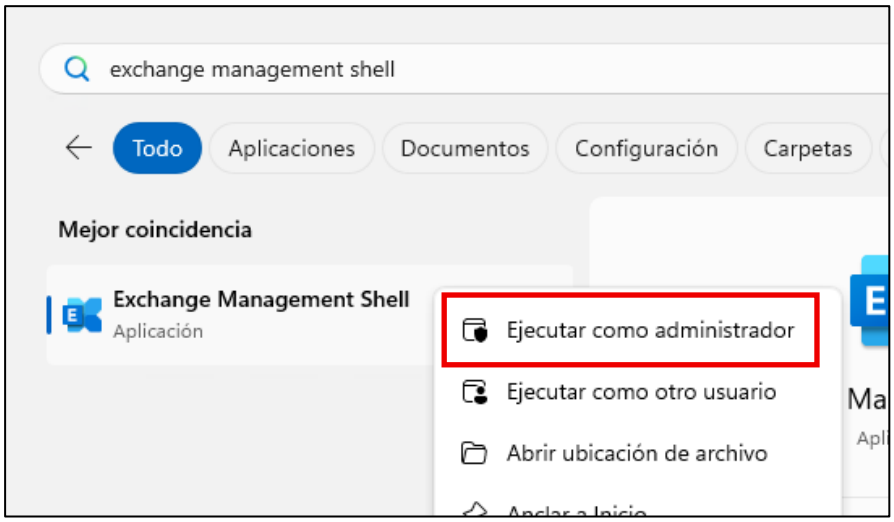


Ilustración 140 - Ejecución como administrador

34.	Introduzca el siguiente comando para habilitar todas las opciones.
	> Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn -ErrorAction SilentlyContinue

```
[PS] C:\WINDOWS\system32>Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn -Error
Action SilentlyContinue
[PS] C:\WINDOWS\system32>
```

Ilustración 141 - Adición de SnapIn

35.	Introduzca el siguiente comando para comprobar el buzón del segundo usuario de pruebas.

```
[PS] C:\WINDOWS\system32>Get-MessageTrackingLog -Recipients "prueba.buzo
nes2@dominio.local" -Start (Get-Date).AddMinutes(-15) -End (Get-Date)
```

Ilustración 142 - Comprobación del buzón

36.	En la salida, deberá ver eventos como “RECEIVE”.

Timestamp	EventId	Source	Sender	Recipients	MessageSubject
04/12/2025 6:00:07	HAREDIRECTFAIL	SMTP	prueba.buzones1@domi...	{prueba.buzones2@dom...	Prueba
04/12/2025 6:00:07	RECEIVE	SMTP	prueba.buzones1@domi...	{prueba.buzones2@dom...	Prueba
04/12/2025 6:00:19	AGENTINFO	AGENT	prueba.buzones1@domi...	{prueba.buzones2@dom...	Prueba
04/12/2025 6:00:35	DEFER	SMTP	prueba.buzones1@domi...	{prueba.buzones2@dom...	Prueba
04/12/2025 6:05:45	SEND	SMTP	prueba.buzones1@domi...	{prueba.buzones2@dom...	Prueba
04/12/2025 6:05:45	DELIVER	STOREDRIVER	prueba.buzones1@domi...	{prueba.buzones2@dom...	Prueba

Ilustración 143 - Visualización de los eventos

37.	De esta manera, queda comprobada la conectividad fundamental.

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL