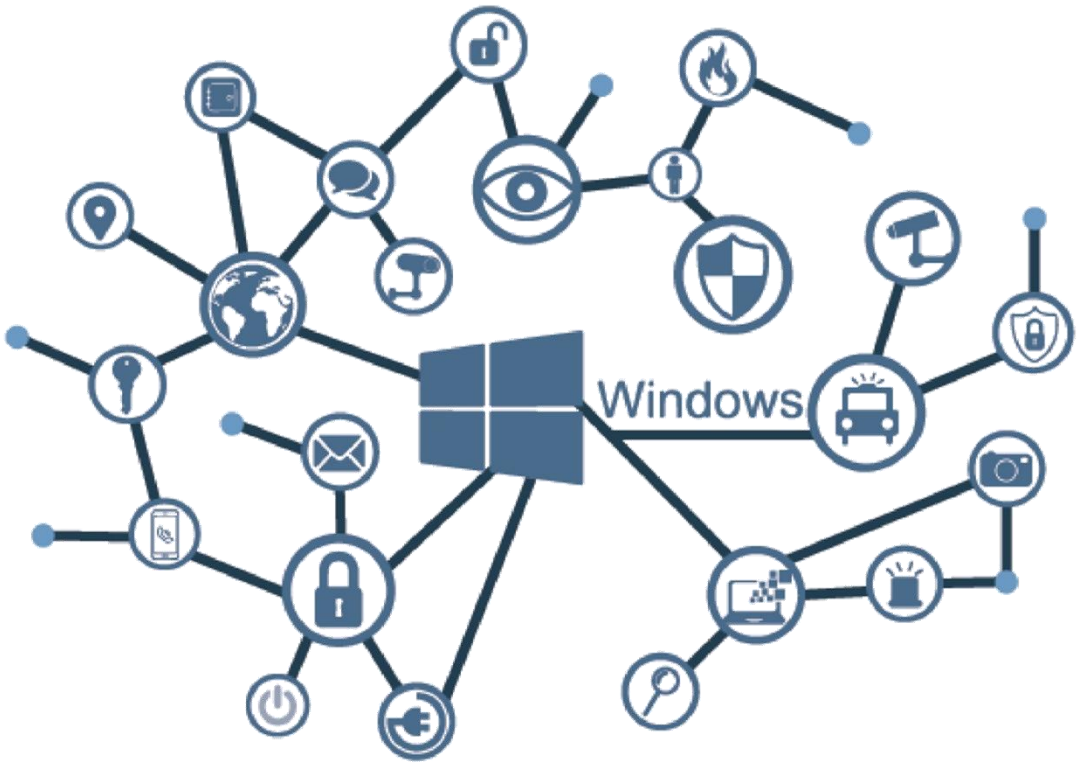
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 577A25

APLICACIÓN DE SEGURIDAD SOBRE MICROSOFT SHAREPOINT SERVER SUBSCRIPTION EDITION



MARZO 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 14:18:21 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO 083-26-273-6 (edición en línea)

Fecha de Edición: marzo 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

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 obligatorio 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, 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 Sharepoint 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-577A25 sobre Microsoft SharePoint, aplicable a los servidores que alojarán el servicio de Sharepoint.

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 Sharepoint 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 Sharepoint 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 basa, 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 (Communication and Information System, 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.

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

3. ALCANCE

La presente guía se ha elaborado para proporcionar información específica para realizar una implementación de la solución de Microsoft Sharepoint 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-577A25 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 2025.

d) Dos servidores miembros del dominio basados en Windows Server 2025.

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

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

   a. Servidor SQL que albergará las bases de datos de Sharepoint, basado en Windows Server 2025.

   b. Servidor Sharepoint único, que mantendrá todos los roles del producto, basado en Windows Server 2025.

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 Sharepoint Subscription Edition. Descripción completa de los mecanismos de seguridad, autenticación y autorización utilizados en Microsoft Sharepoint Subscription Edition.

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 Sharepoint 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 Sharepoint Subscription Edition, será necesario verificar:
    - Compatibilidad del sistema operativo (Windows Server en la versión soportada por Microsoft Sharepoint Subscription Edition).
    - Configuración de hardware mínima.
    - Versiones y parches actualizados del sistema operativo, seguridad y componentes críticos.
- Requisitos técnicos específicos: Se deben cumplir los requisitos definidos por Microsoft Sharepoint, 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 Sharepoint.

4.2. Instalación y Aplicación de Seguridad sobre rol IIS

Antes de proceder con la instalación de Microsoft Sharepoint 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 Sharepoint. 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 el registro de eventos relevantes.

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

IIS:

a) Activación únicamente de los módulos requeridos por Sharepoint (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 Sharepoint Server 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 Sharepoint.

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 tabla se 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	✗	✗	✓

Tabla 1. Selección de perfil de medidas de seguridad

En los apartados siguientes se desarrollarán los controles específicos aplicables a Microsoft Sharepoint Server 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 Sharepoint 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 Sharepoint Server SE

En el presente anexo se define un marco base para la aplicación de aquellos requisitos de seguridad sobre el servicio Microsoft Sharepoint Server 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 aplicado a un servicio de Microsoft Sharepoint 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 2025.
  - Guía base de aplicación de seguridad utilizada: CCN-STIC-570A25. Perfilado de seguridad para Windows Server (DC o MS).
- **Servidor Sharepoint Server Subscription Edition** (1 servidor):
  - 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: CCN-STIC-574A25 Implementación de Seguridad Microsoft Internet Information Services (IIS) 10.

Nota: Durante la redacción de esta guía se crea una granja de servidor único. Este rol determinará que todos servicios de Sharepoint se ejecutarán en este servidor. Para entornos productivos, se recomienda utilizar roles dedicados o compartidos, cuya optimización mejora el rendimiento y la escalabilidad del servicio. En ese caso, es importante estudiar la aplicabilidad de las guías anteriores.

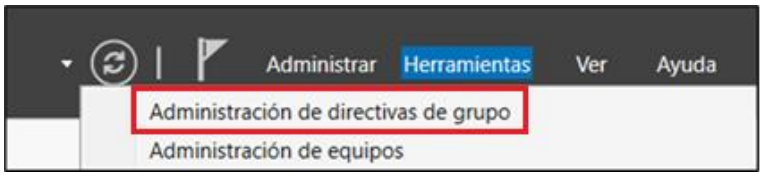
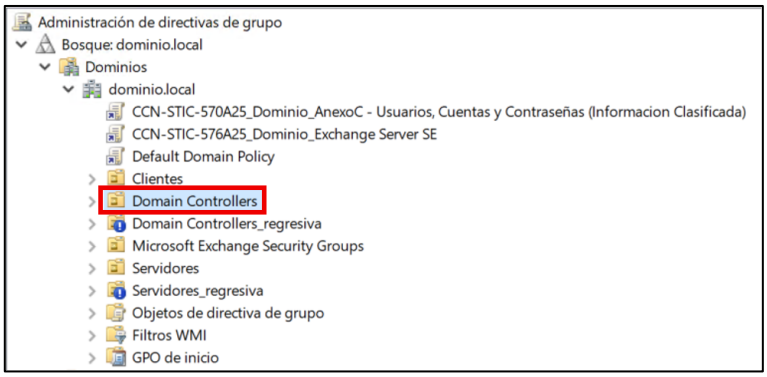
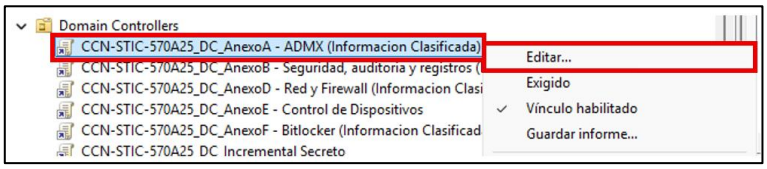
- **Servidor de base de datos SQL Server (1 servidor):**
  - Sistema operativo: Windows Server 2025.
  - Guía base de aplicación de seguridad utilizada:
  - CCN-STIC-575 Implementación de seguridad en MS SQL Server 2016 sobre MS Windows Server 2016.
  - CCN-STIC-570A25. Perfilado de seguridad para Windows Server (DC o MS).

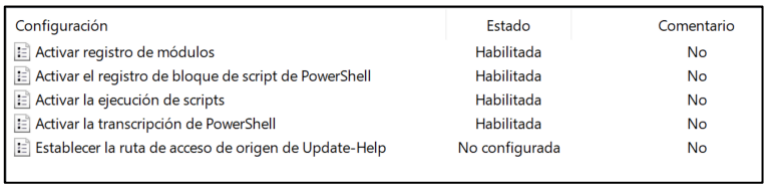
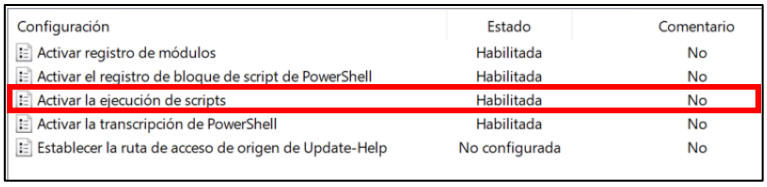
Nota: Es importante destacar que las guías de seguridad mencionadas han sido aplicadas sobre los servidores involucrados tras la completa configuración del servicio de Sharepoint Server Subscription Edition. Antes de aplicar cada una de ellas, será necesario analizar las configuraciones que se implementarán, con el objetivo de no impactar en los prerrequisitos de dicho producto.

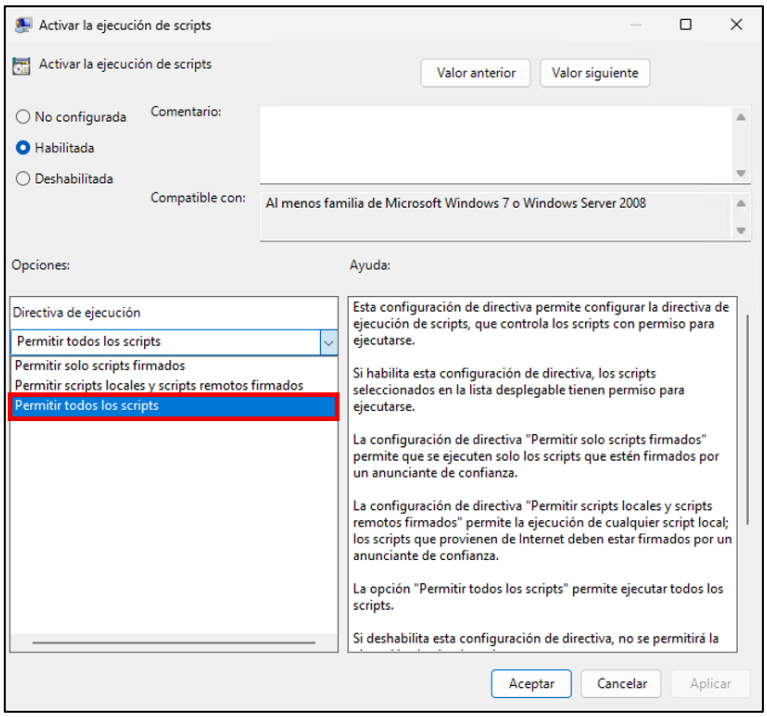
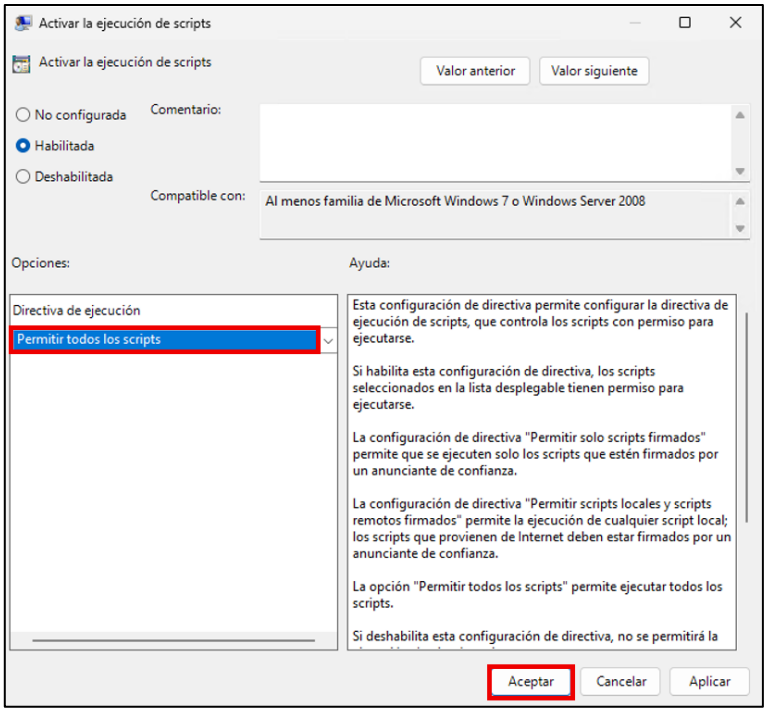
El usuario administrador del dominio que se utilice para todas las tareas descritas en la presente operativa deberá pertenecer a los siguientes grupos:

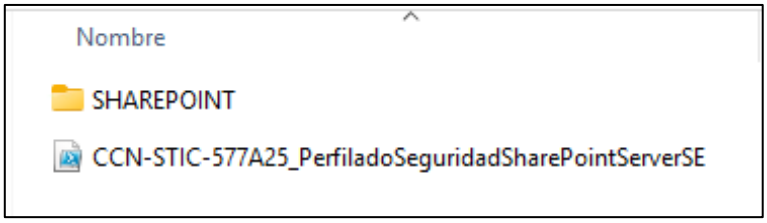
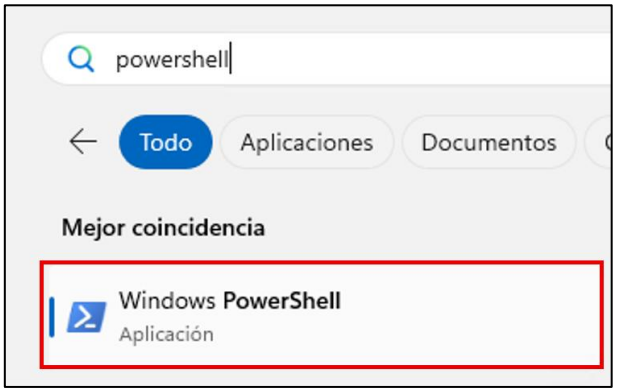
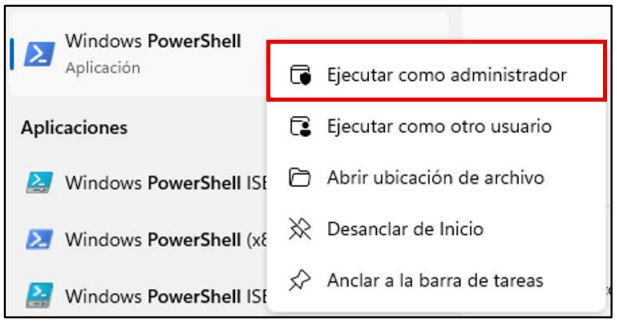
- Administradores.
- Administradores de empresas.
- Administradores de esquema.
- Admins. de dominio.
- Organization Manager.
- Propietarios del creador de directivas de grupo.
- Usuarios del dominio.

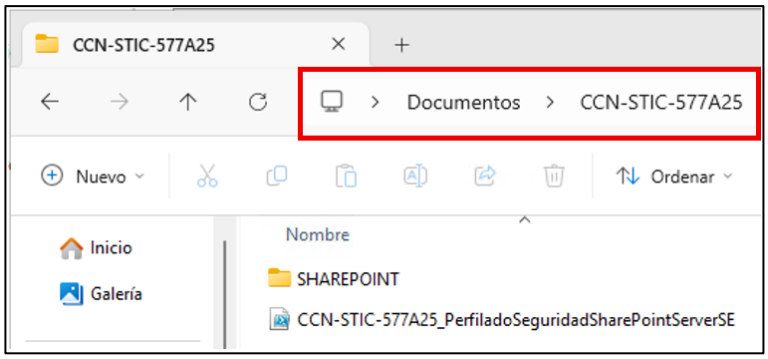
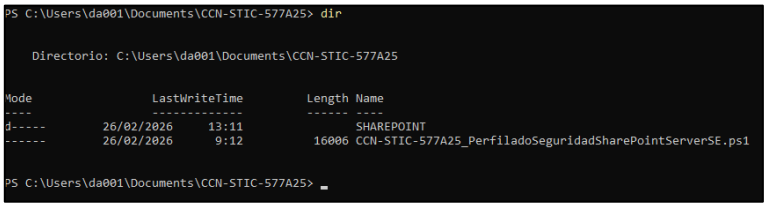
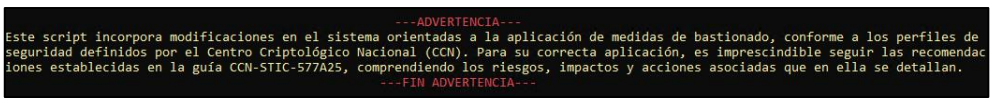
ANEXO A.1. Implementación de Políticas de Seguridad sobre el Dominio

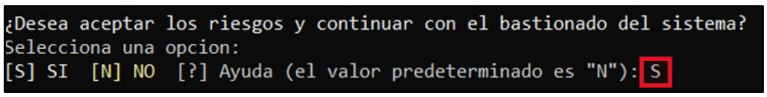
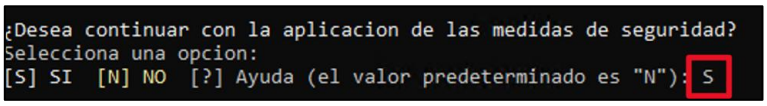
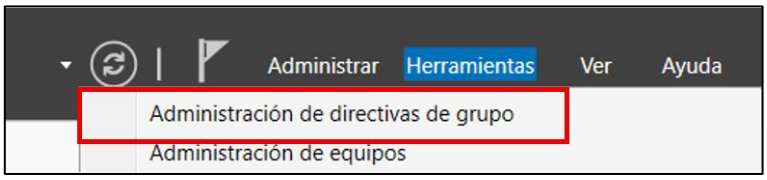
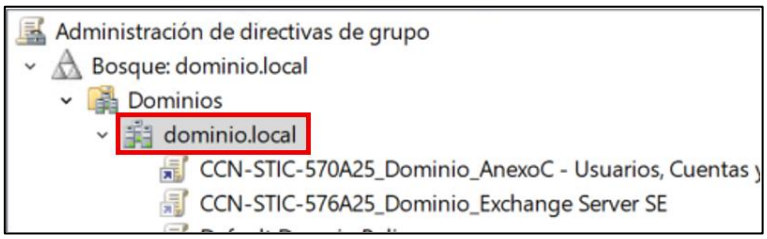
Paso	Descripción
1.	Inicie sesión con un usuario miembro del grupo Admins. de Dominio en un Controlador de Dominio.
2.	En el "Administrador del servidor", haga clic en "Herramientas" en la barra superior y seleccione "Administración de directivas de grupo".  *Ilustración 1 - Administración de directivas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

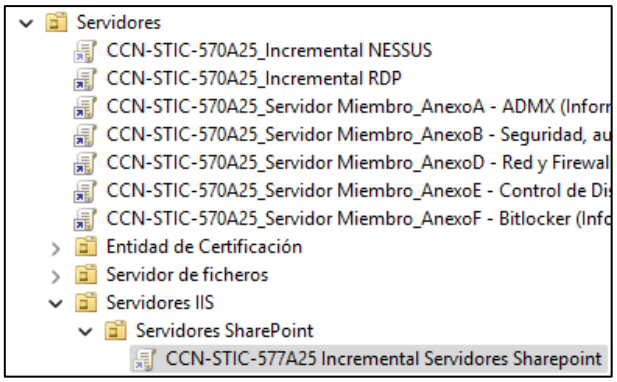
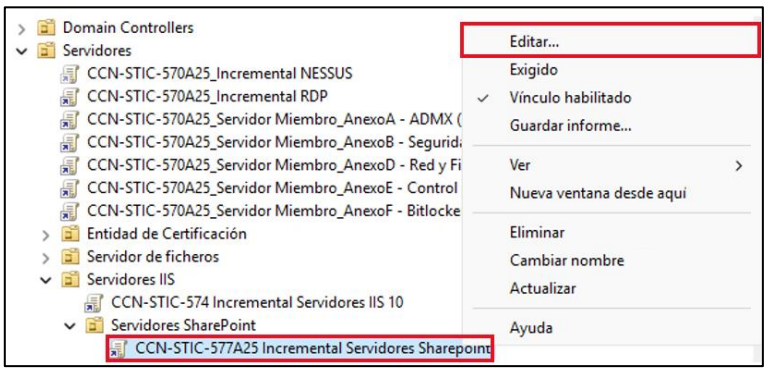
5.	En el panel “Editor de administración de directivas de grupo”, despliegue la lista siguiendo la siguiente ruta: “Configuración del Equipo > Plantillas administrativas > Componentes de Windows > Windows PowerShell”. Haga clic sobre “Windows PowerShell” para consultar las políticas que aplica.  *Ilustración 4 - Políticas de PowerShell*
6.	Haga doble clic sobre la política “Activar la ejecución de scripts”.  *Ilustración 5 - Activar la ejecución de scripts*

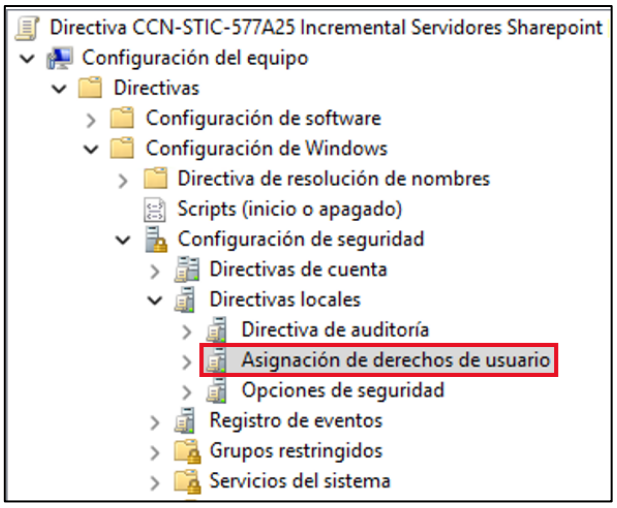
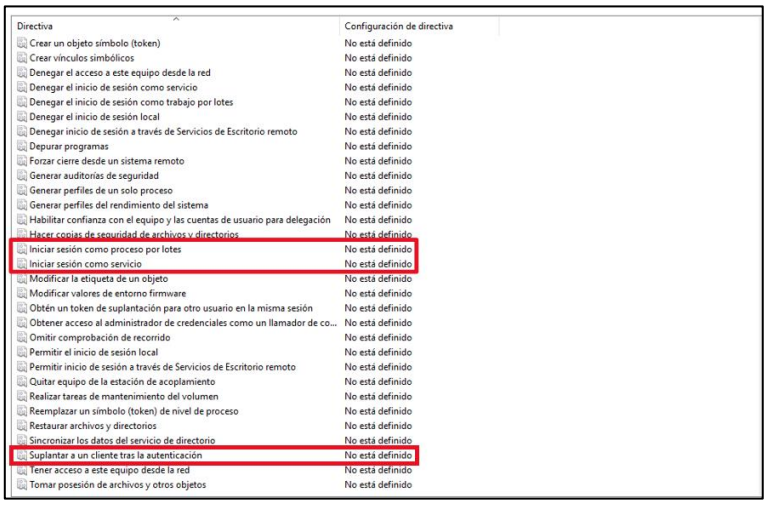
7.	En el desplegable de la política, seleccione “Permitir todos los scripts”:  *Ilustración 6 - Selección de "Permitir todos los scripts"*
8.	A continuación, pulse en “Aplicar” y “Aceptar”  *Ilustración 7 – Confirmación de cambios.*
9.	Reinicie el controlador de dominio para que se aplique la configuración correctamente.

10.	En el controlador de dominio, copie los ficheros y directorios que acompañan a esta guía al directorio "Documentos" del usuario administrador. A continuación, descomprima la carpeta. Verifique que en su interior se encuentran los siguientes archivos: - Directorio: SHAREPOINT - Fichero: CCN-STIC-577A25_PerfiladoSeguridadSharepointServerSE.ps1  *Ilustración 8 - Copia de ficheros necesarios*
11.	Sobre la barra de búsqueda, escriba "PowerShell":  *Ilustración 9 - Windows PowerShell*
12.	Haga clic derecho, y seleccione "Ejecutar como administrador":  *Ilustración 10 - 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.

13.	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 11 - Copia de ruta*
14.	Desde la ventana de PowerShell, utilizando el comando “cd”, acceda a la ruta recientemente copiada.  *Ilustración 12 - Acceso a la ruta*
15.	Ejecute el comando “dir” para verificar la ubicación y el contenido.  *Ilustración 13 - Contenido de la carpeta*
16.	Ejecute el archivo “CCN-STIC577A25_PerfiladoSeguridadSharepointServerSE.ps1” escribiendo “.\” y pulsando la tecla tabuladora hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución.  *Ilustración 14 - Ejecución del script*
17.	A continuación, se mostrará una advertencia de uso, continuando con el siguiente mensaje:  *Ilustración 15 - Advertencia*

18.	Escribir “S” y pulsar “Enter”.  *Ilustración 16 - Aceptación de advertencia*
19.	Se realizará una comprobación para confirmar si el dominio dispone de una unidad organizativa preparada para los servidores IIS. En caso de no existir, se creará automáticamente. Para continuar, introduzca “S” y pulsar “Enter”.  *Ilustración 17 - Selección de configuración*
20.	Puede cerrar la consola de PowerShell.
21.	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*
22.	Expanda la lista del menú izquierdo hasta llegar al dominio, y haga clic sobre él para desplegarlo.  *Ilustración 19 - Selección de dominio*

23.	Como puede observar, quedará creada la unidad organizativa “Servidores Sharepoint” y la directiva correspondiente asociada y pendiente de vincular.  *Ilustración 20 - Unidad organizativa "Servidores Sharepoint"*
24.	A continuación, pulse con el botón derecho sobre la directiva y seleccione “Editar”.  *Ilustración 21 - Edición de directiva de Sharepoint*

25.	Diríjase a “Configuración de equipo > Directivas > Configuración de Windows > Configuración de seguridad > Directivas locales > Asignación de derechos de usuario”.  *Ilustración 22 - Asignación de derechos de usuario*
26.	En el campo de configuraciones, localice los siguientes parámetros: - Iniciar sesión como proceso por lotes. - Iniciar sesión como servicio. - Suplantar a un cliente tras la autenticación.  *Ilustración 23 - Derechos de usuario*

27.	Edite las tres configuraciones haciendo doble clic sobre ellas, y sustituya el usuario por la cuenta de servicio utilizada en el pool de aplicaciones de Sharepoint. A continuación, pulse “Aceptar”.

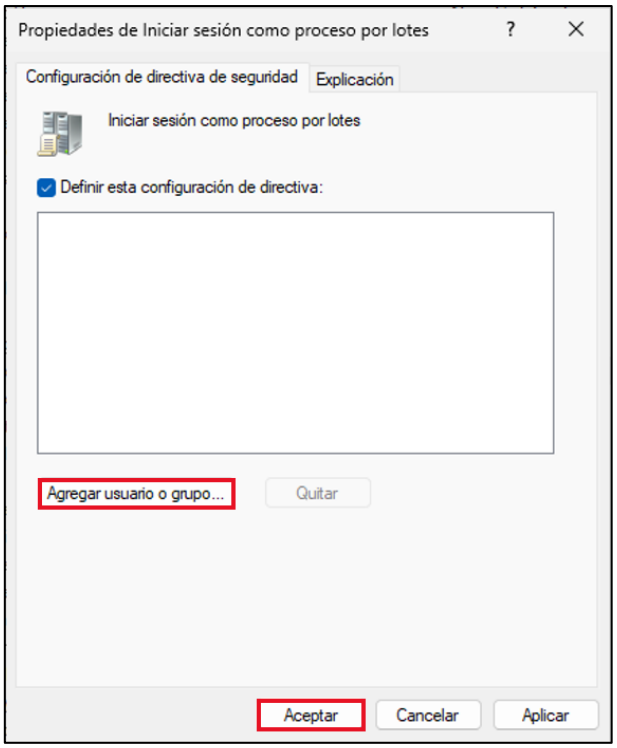


Ilustración 24 - Sustitución de cuenta de servicio

28.	En entornos corporativos con segmentación de redes, la administración de los diferentes componentes se realiza desde redes de administración. Por ello, será necesario habilitar una regla de firewall local para acceder a la consola de administración. En la misma GPO, diríjase a "Configuración de equipo > Directivas > Configuración de Windows > Configuración de seguridad > Windows Defender Firewall con seguridad avanzada > Windows Defender Firewall con seguridad avanzada-LDAP > Reglas de entrada".

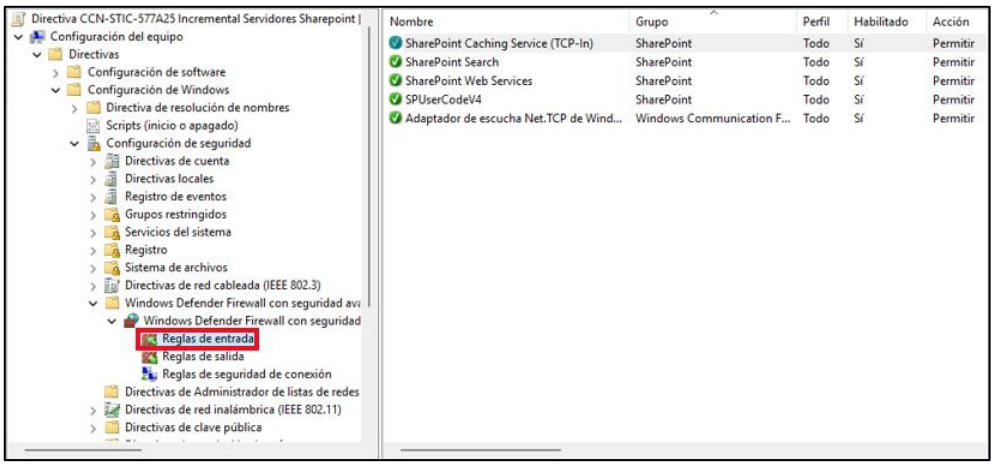


Ilustración 25 - Reglas de entrada de Firewall

29.	Cree una nueva regla que sustituya la actual "Sharepoint Central Administration v4", introduciendo el puerto correspondiente a la administración de su infraestructura. Para ello, pulse con el clic derecho sobre "Reglas de entrada" y seleccione "Nueva regla".

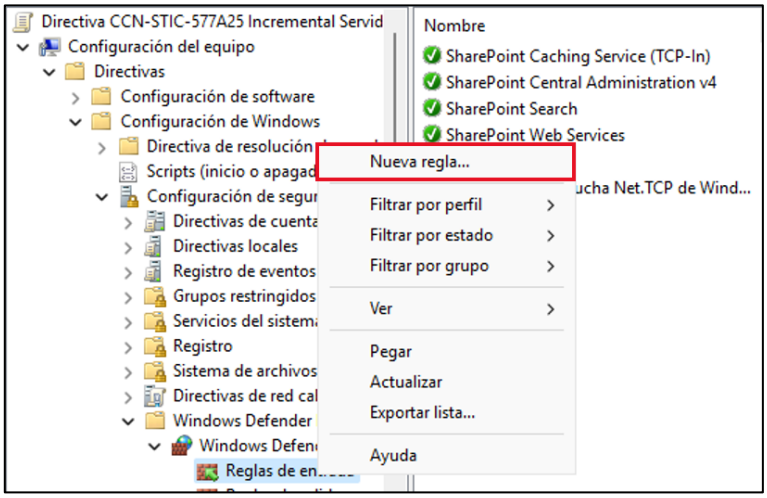


Ilustración 26 - Nueva regla de Firewall

30.	Seleccione "Puerto" en el asistente de configuración de nueva regla y a continuación, pulse en "Siguiente".

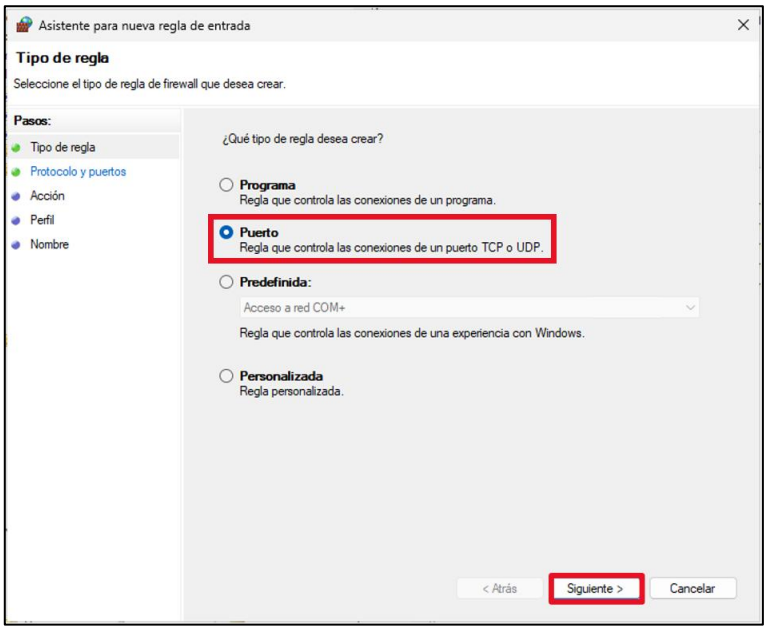


Ilustración 27 - Selección de opciones de regla

31. Asegúrese que la opción TCP se encuentra marcada e introduzca el puerto de administración de su granja de Sharepoint. Tras ello, haga clic en “Siguiente”.

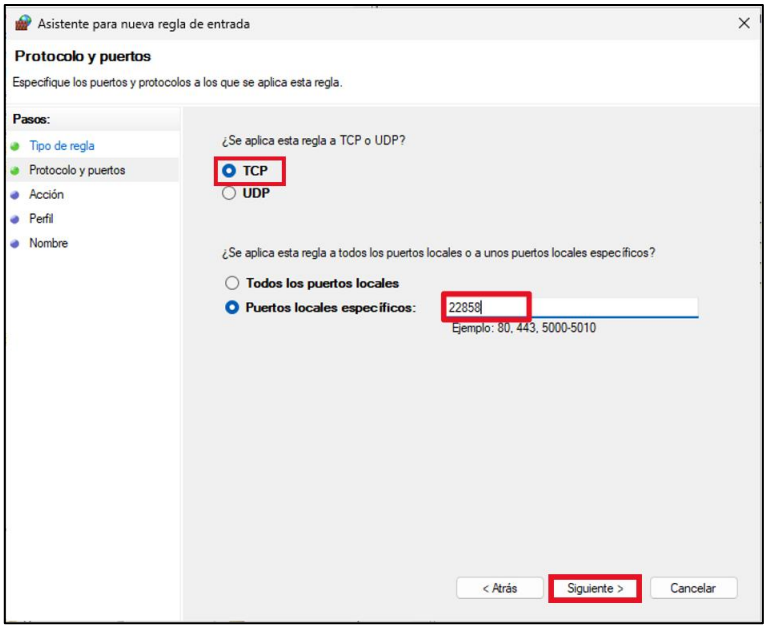


Ilustración 28 - Introducción de puerto de administración

32.	A continuación, pulse en “Siguiente” para permitir la conexión remota al puerto indicado.

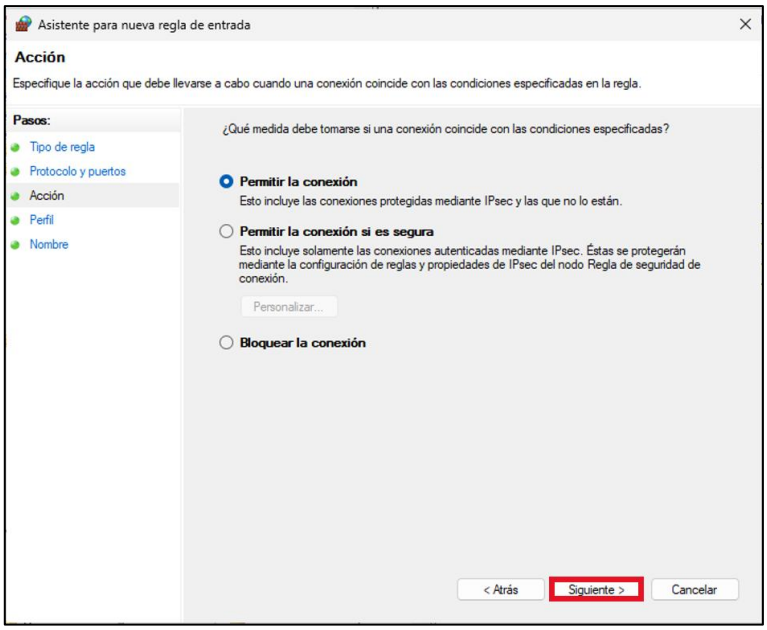


Ilustración 29 - Asistente de creación de regla

33.	Del mismo modo, haga clic en “Siguiente” manteniendo la aplicación de la regla para los diferentes entornos.

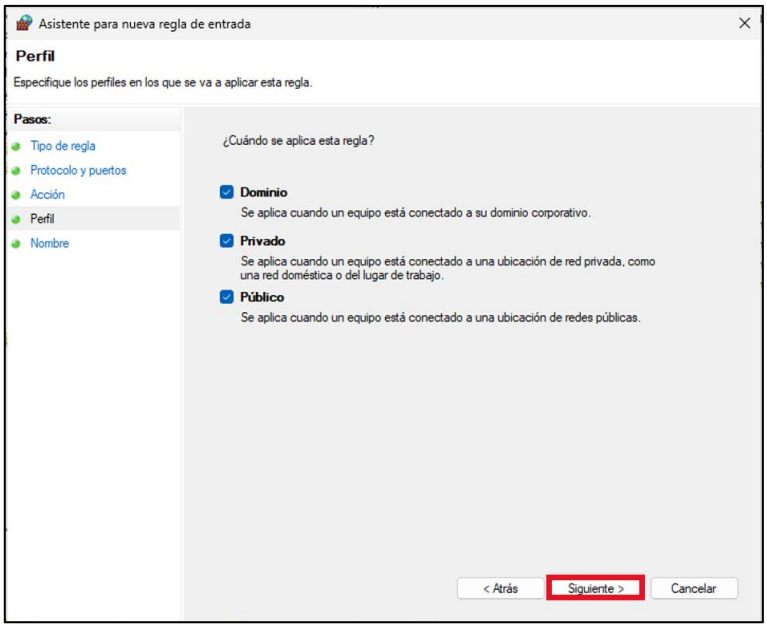
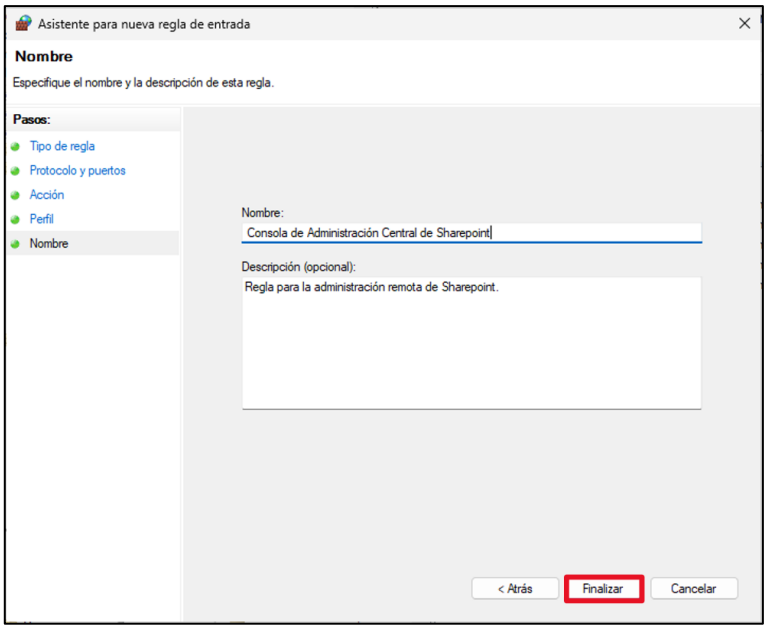
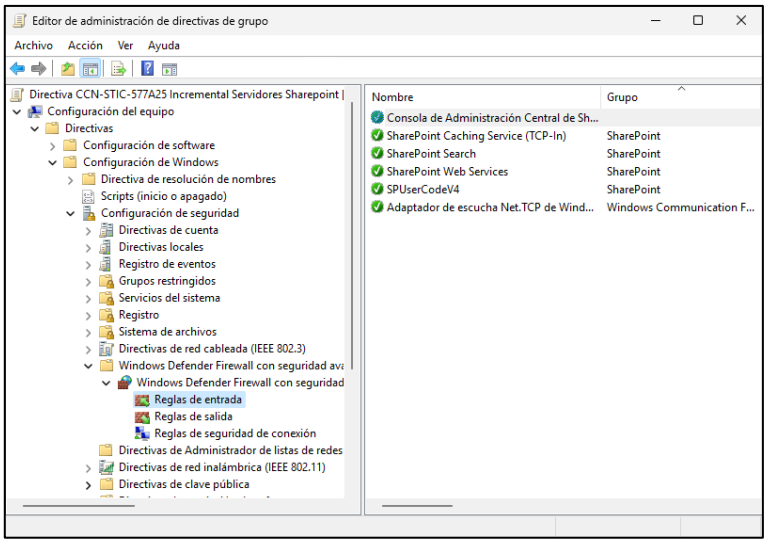


Ilustración 30 - Selección de aplicación de regla

34.	Indique un nombre descriptivo y un resumen de la regla, y a continuación, pulse en “Finalizar”.  *Ilustración 31 - Creación de regla de Firewall*
35.	De este modo, la regla que permite el acceso a la administración de Sharepoint quedará configurada.  *Ilustración 32 - Reglas de Firewall* **Nota**: Si la administración de la granja de servidores de Sharepoint se realiza en el propio servidor frontal del servicio, no será necesario realizar esta acción.
36.	A continuación, cierre ventana de configuración de la directiva.

37.	Haga clic con el botón derecho sobre la directiva "CCN-STIC-577A25 Incremental Servidores Sharepoint" y, a continuación, seleccione "Vínculo habilitado".

Ilustración 33 - Habilitación de vínculo

38.	De nuevo en el "Administrador del servidor", haga clic en "Herramientas" en la barra superior, y seleccione "Usuarios y equipos de Active Directory".

Ilustración 34 - Usuarios y equipos de Active Directory

39.	Despliegue la lista del panel izquierdo hasta visualizar la OU "Servidores Sharepoint".

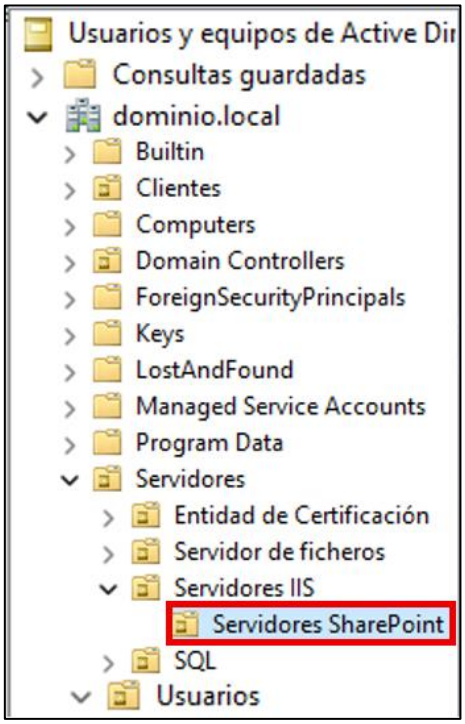
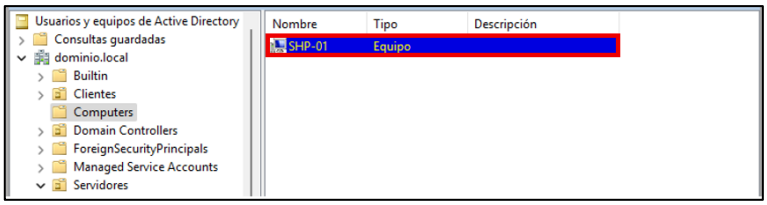
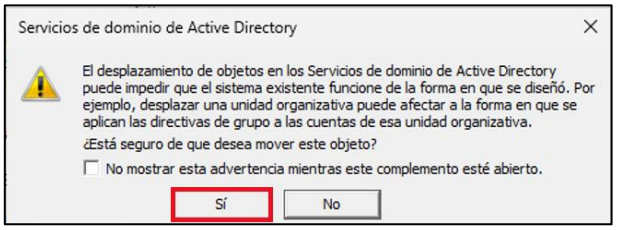
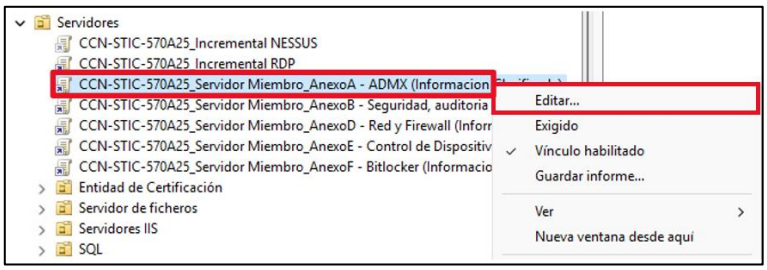
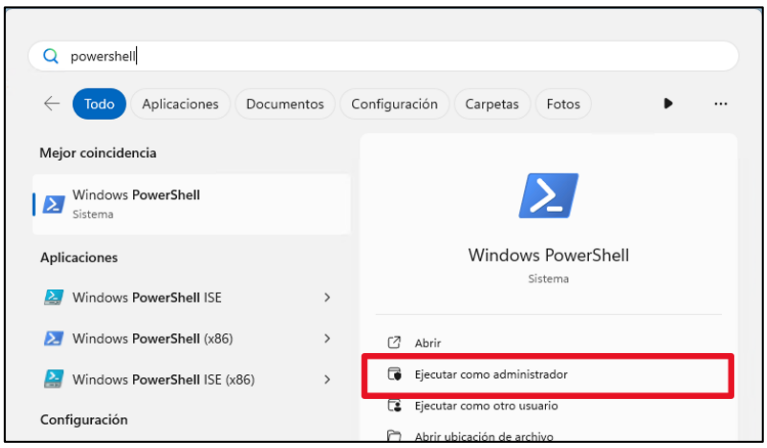
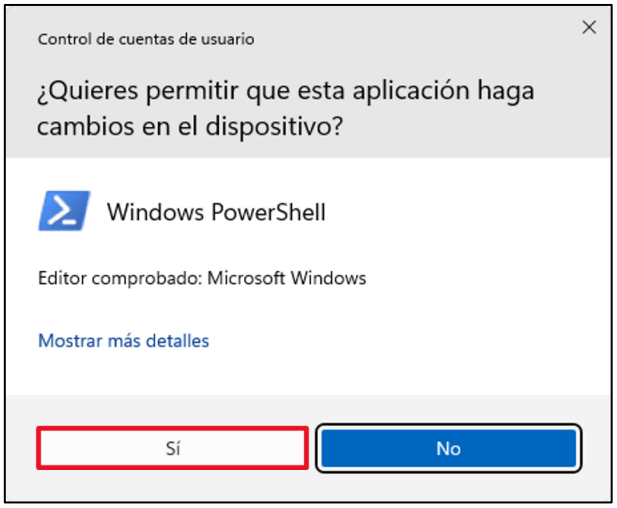
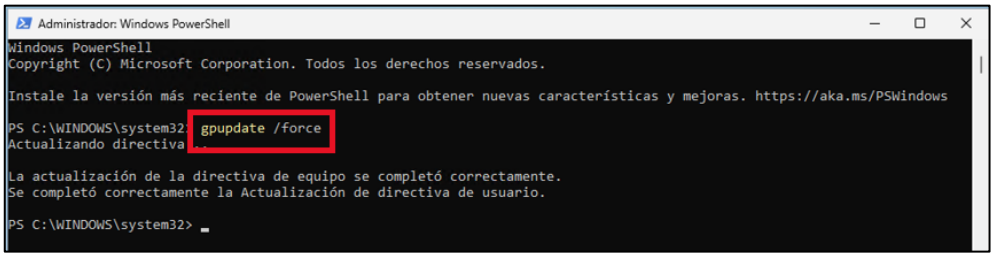
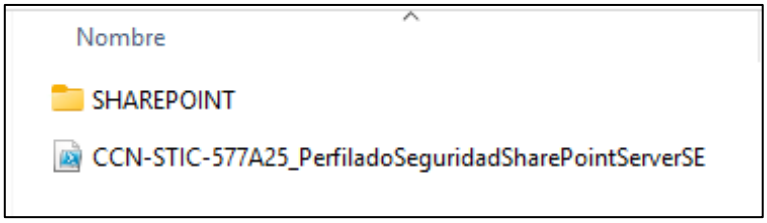
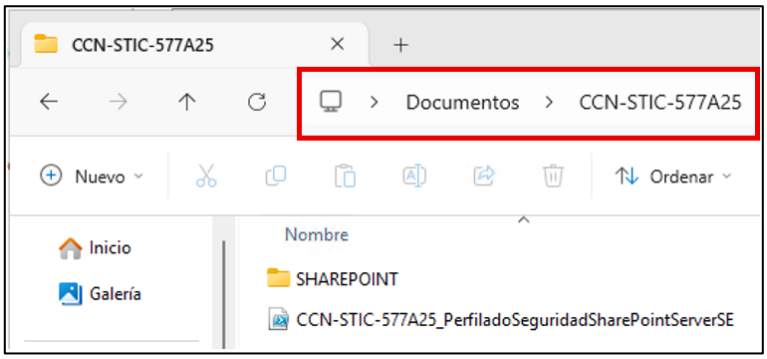
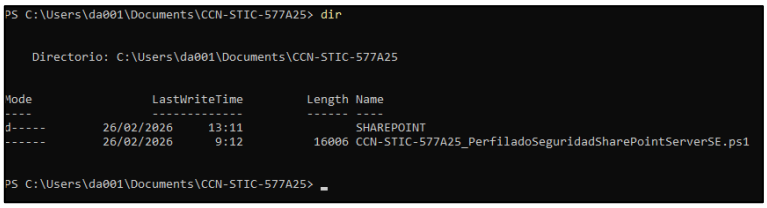
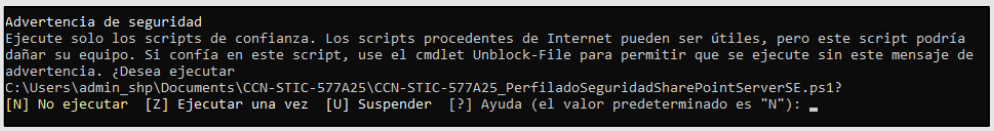
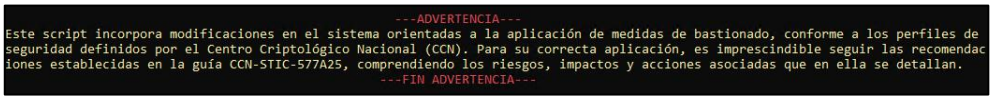
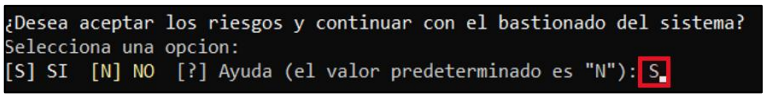


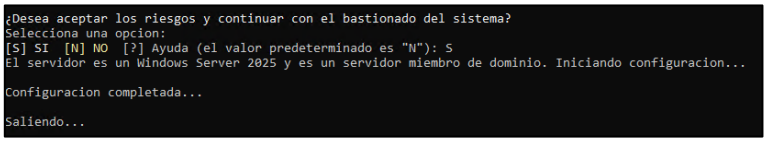
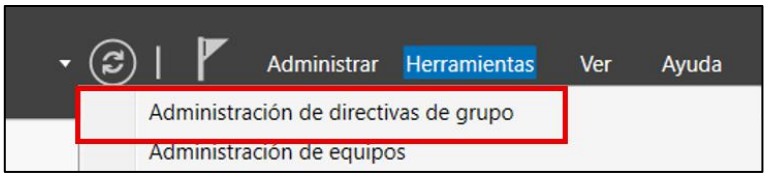
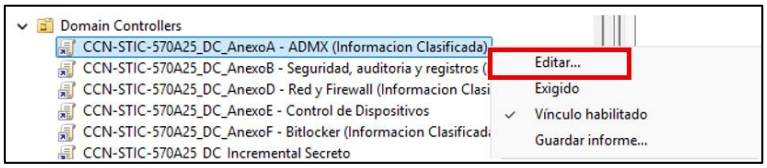
Ilustración 35 - OU Servidores Sharepoint SE

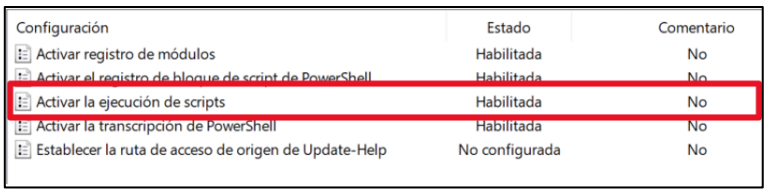
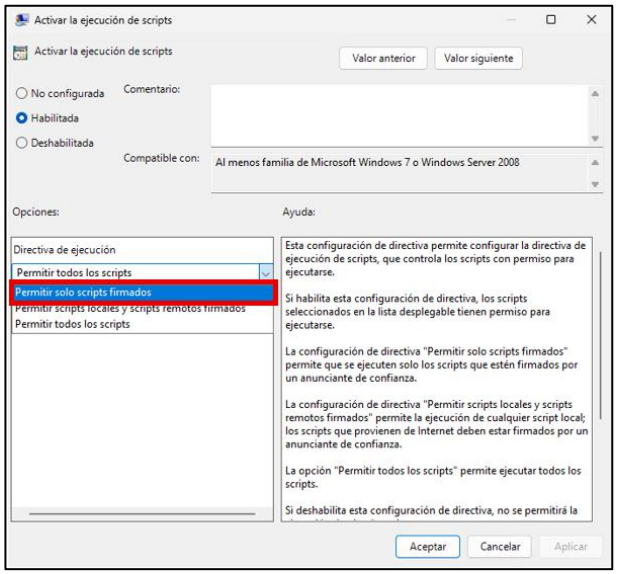
40.	Haga clic sobre la carpeta “Computers” y seleccione el servidor Sharepoint Server SE.  *Ilustración 36 - Selección de los servidores*
41.	Arrástrelo a la OU “Servidores Sharepoint”. Aparecerá una advertencia. Haga clic en “Sí”.  *Ilustración 37 - Advertencia tras el movimiento de servidores*
42.	A continuación, comenzará la aplicación de las medidas de seguridad en el servidor de Sharepoint. Para ello, edite la GPO de Servidor Miembro para permitir la ejecución de scripts siguiendo los pasos iniciales de este procedimiento. En la consola de administración de directivas de grupo, haga clic con el botón derecho y edite la política “CCN-STIC-570A25_Servidor Miembro_AnexoA – ADMX (Información Clasificada)”.  *Ilustración 38 - Edición de directiva de Servidor Miembro*
43.	A continuación, inicie sesión en el servidor Sharepoint con un usuario con privilegios de administración.

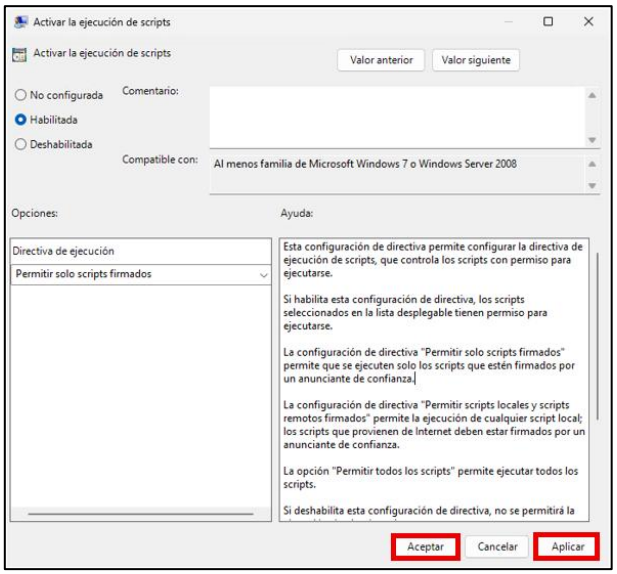
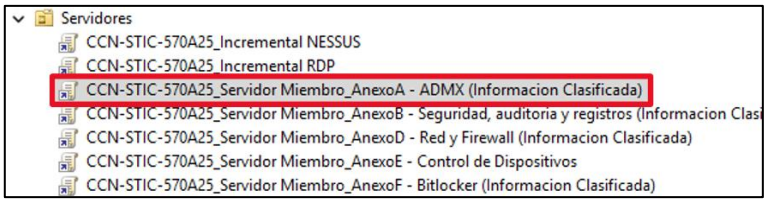
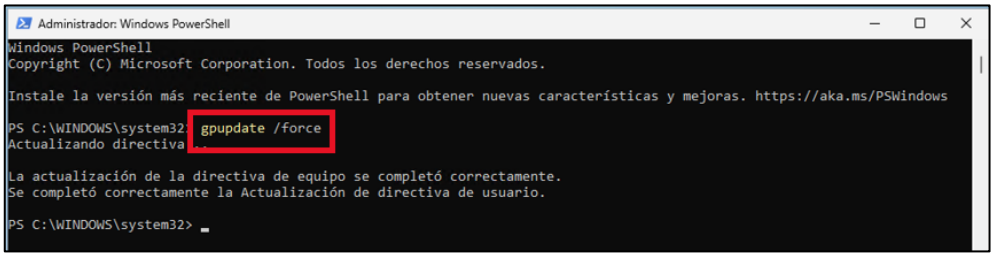
44.	Pulse el botón de inicio y a continuación, escriba “Powershell”. Haga clic sobre “Ejecutar como administrador”.  *Ilustración 39 - Ejecución de Powershell*
45.	Pulse en “Sí” para confirmar la ejecución de la herramienta.  *Ilustración 40 - Aceptar ejecución de Powershell*
46.	Escriba el comando “gpupdate /force” para aplicar las directivas vinculadas a su nueva unidad organizativa.  *Ilustración 41 - Ejecución del comando*
47.	Proceda a reiniciar la máquina y, de nuevo, inicie sesión con un usuario con privilegios de administración del servidor.

48.	Copie los ficheros y directorios que acompañan a esta guía en la carpeta "Documentos" del usuario administrador. A continuación, descomprima la carpeta. Verifique que en su interior se encuentran los siguientes archivos: - Directorio: SHAREPOINT - Fichero: CCN-STIC-577A25_PerfiladoSeguridadSharepointServerSE.ps1  *Ilustración 42 - Archivos copiados*
49.	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 43 - Copia de ruta*
50.	Desde la ventana de PowerShell, utilizando el comando "cd", acceda a la ruta recientemente copiada.  *Ilustración 44 - Acceso al directorio*

51.	Ejecute el comando “dir” para verificar la ubicación y el contenido.  *Ilustración 45 - Contenido de la carpeta*
52.	Ejecute el archivo “CCN-STIC577A25_PerfiladoSeguridadSharepointServerSE.ps1” escribiendo “.\” y pulsando la tecla tabuladora hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución.  *Ilustración 46 - Ejecución del script* **Nota**: Si le aparece una advertencia similar a la mostrada en la siguiente imagen, pulse la tecla “Z” y posteriormente, “Enter”.  *Ilustración 47 - Advertencia de ejecución de scripts*
53.	A continuación, se mostrará una advertencia de uso, continuando con el siguiente mensaje:  *Ilustración 48 - Advertencia de seguridad*
54.	Escribir “S” y pulsar “Enter”.  *Ilustración 49 - Aceptación de advertencia*

55.	Si el servidor ha sido bastionado con la guía CCN-STIC-574A25, el script realizará los cambios correspondientes para que el funcionamiento sea correcto.  *Ilustración 50 - Finalización del script*
56.	Puede cerrar la consola de Powershell.
57.	A continuación, restablezca la configuración de la ejecución de scripts en los equipos. Inicie sesión con un usuario perteneciente al grupo Admins. del Dominio en un Controlador de Dominio.
58.	En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.  *Ilustración 51 - Administración de directivas de grupo*
59.	Despliegue el panel izquierdo hasta llegar a la OU “Domain Controllers”.  *Ilustración 52 - OU Domain Controllers*
60.	Despliegue dicha OU, haga clic derecho sobre la GPO “CCN-STIC-570A25_DC_AnexoA – ADMX (Nivel de Clasificación)”, y seleccione “Editar”.  *Ilustración 53 - Edición ADMX 570A25*

61.	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 54 - Políticas de PowerShell*
62.	Haga doble clic sobre la política “Activar la ejecución de scripts”.
63.	En el desplegable de la política, seleccione “Permitir solo scripts firmados”.  *Ilustración 55 - Selección de "Permitir solo scripts firmados"*

64.	A continuación, pulse en “Aplicar” y “Aceptar”.  *Ilustración 56 - Aplicación de la política*
65.	Realice las mismas acciones para la directiva “CCN-STIC-570A25_Servidor Miembro_AnexoA – ADMX (Informacion Clasificada)”.  *Ilustración 57 - Edición de directiva de servidor miembro*
66.	A continuación, ejecute el comando “gpupdate /force” en el controlador de dominio y servidor de Sharepoint.  *Ilustración 58 - Ejecución del comando*
67.	Reinicie ambos servidores para que se aplique la configuración correctamente.

ANEXO A.2. Configuraciones Adicionales

El presente anexo se desarrolla con el objetivo de recoger aquellas configuraciones adicionales de seguridad asociadas a un riesgo concreto, las cuales no pueden ser aplicadas por medio de configuraciones a nivel de Windows, ya sea por su naturaleza específica o dependencias del entorno.

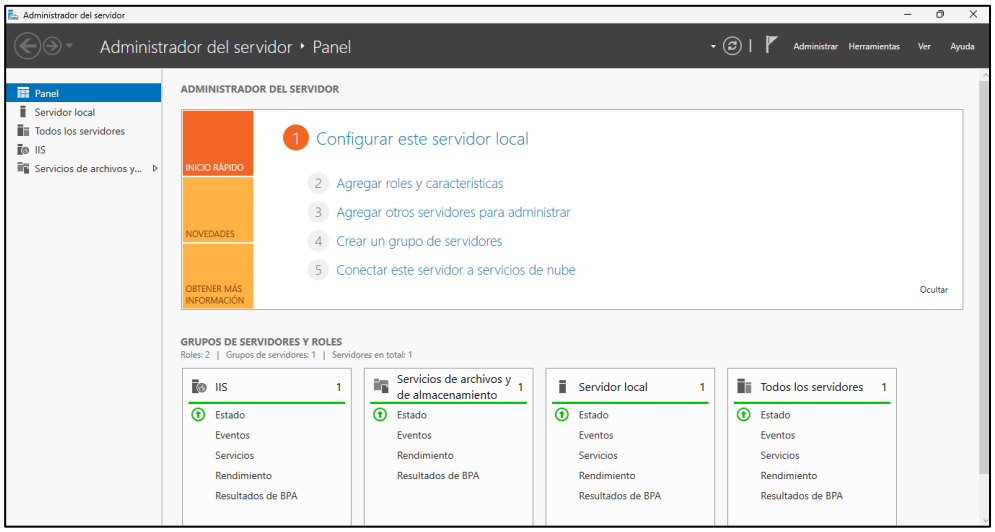
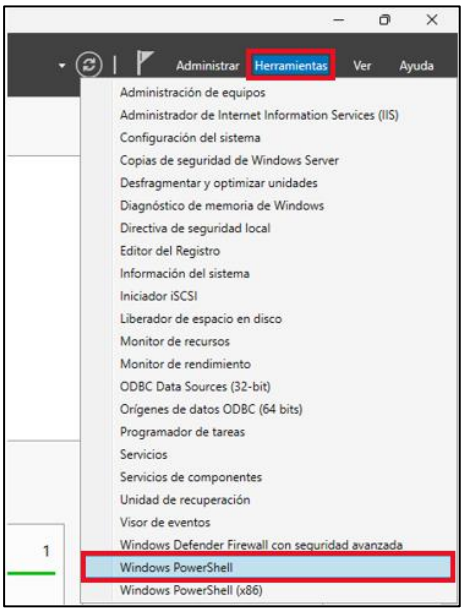
Este apartado recoge las directivas adicionales y ajustes de seguridad necesarios para garantizar la integridad y la protección del servicio de SharePoint Server. Por el contrario, no hará referencia a la configuración paso a paso de otras recomendaciones y buenas prácticas detalladas por el fabricante que cabe destacar. Para fortalecer la arquitectura, se recomienda la implementación del modelo MinRole, ya que dicha tecnología no solo optimiza el rendimiento, si no que facilita la segregación de roles reduciendo la superficie de exposición. A su vez, en esa misma línea de aislamiento es fundamental segregar el tráfico de red entre las principales capas de la infraestructura, priorizando la segmentación entre los roles principales de Sharepoint y los servidores SQL Server aplicando reglas estrictas de comunicaciones. Del mismo modo, por razones de seguridad perimetral, es altamente recomendable no exponer la consola de administración central en redes de clientes o DMZ en escenarios donde el frontal se encuentre accesible desde dichas redes.

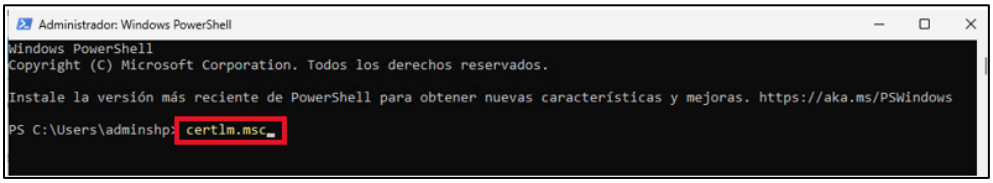
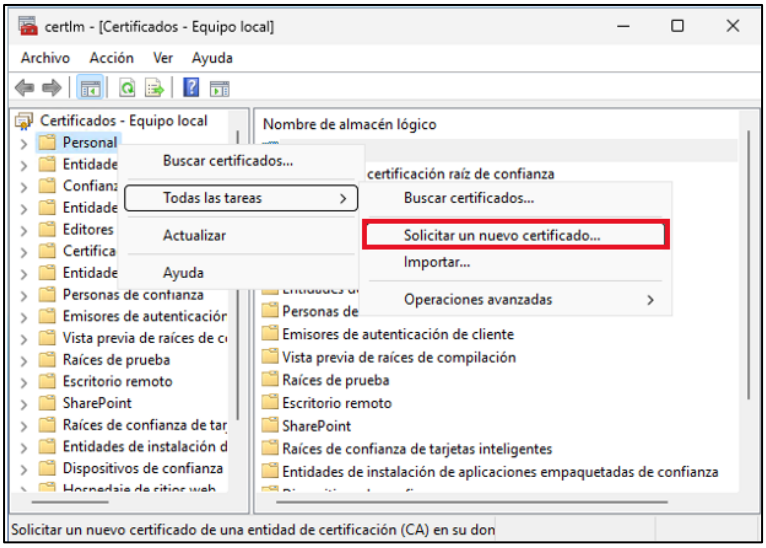
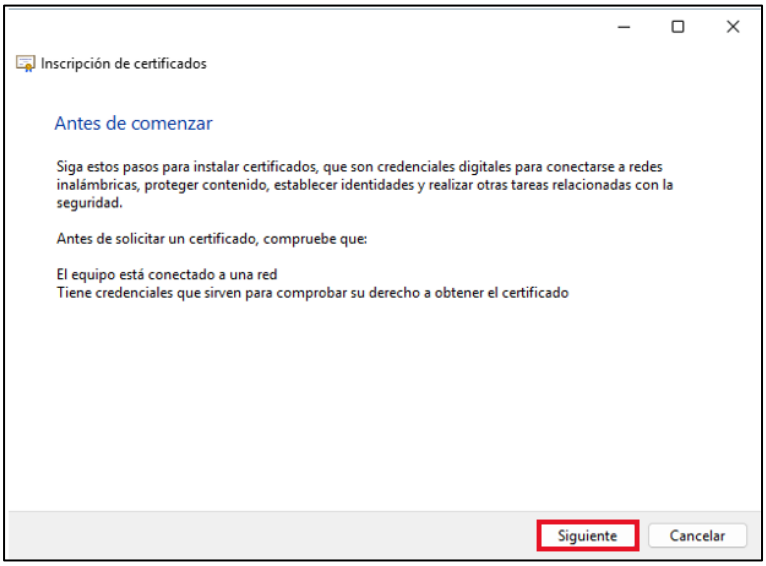
Por otro lado, se considera necesario el diseño e implementación de controles de versiones con el objetivo de mitigar el riesgo de pérdida de información, permitir la trazabilidad de cambios y facilitar la recuperación ante borrados o corrupción de archivos. Dicha trazabilidad, deberá apoyarse en una supervisión activa de la actividad de los usuarios mediante roles de administración y auditoría, así como la exportación de logs de los diferentes elementos a sistemas de gestión de eventos externos.

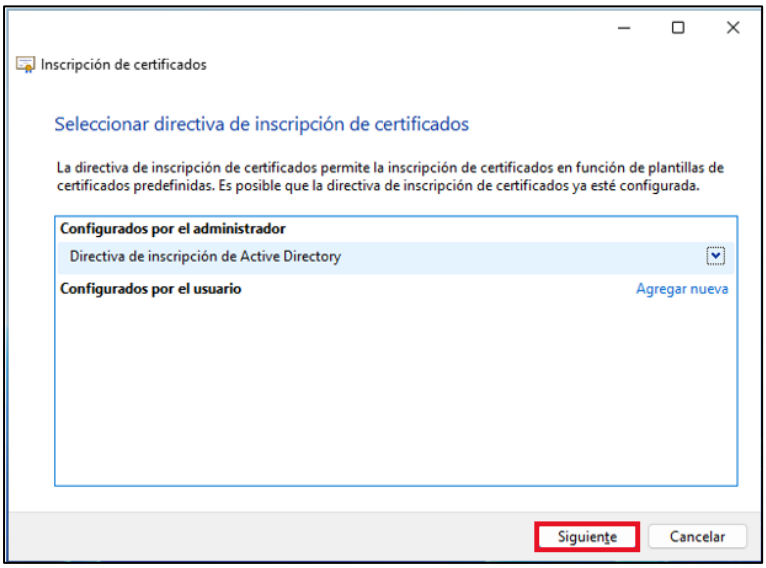
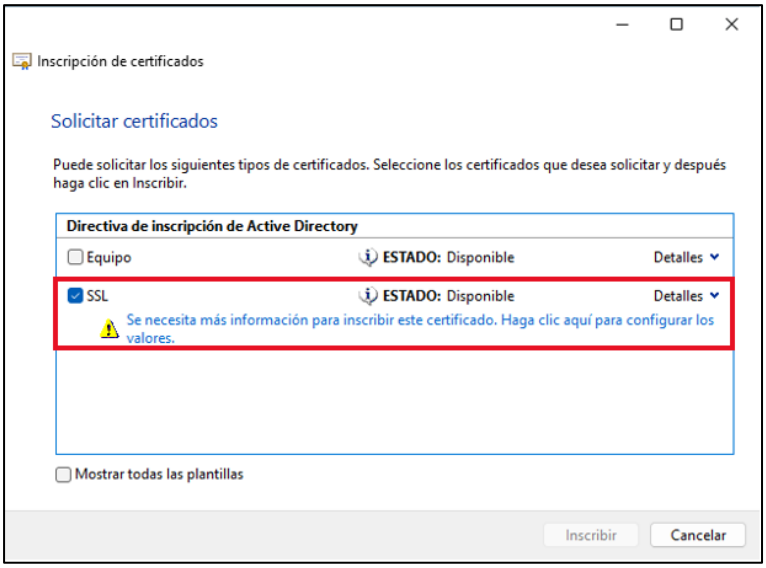
ANEXO A.2.1. Certificados

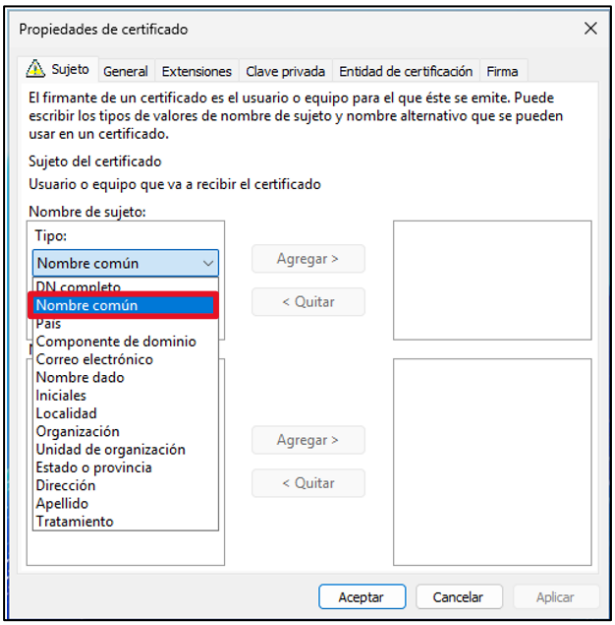
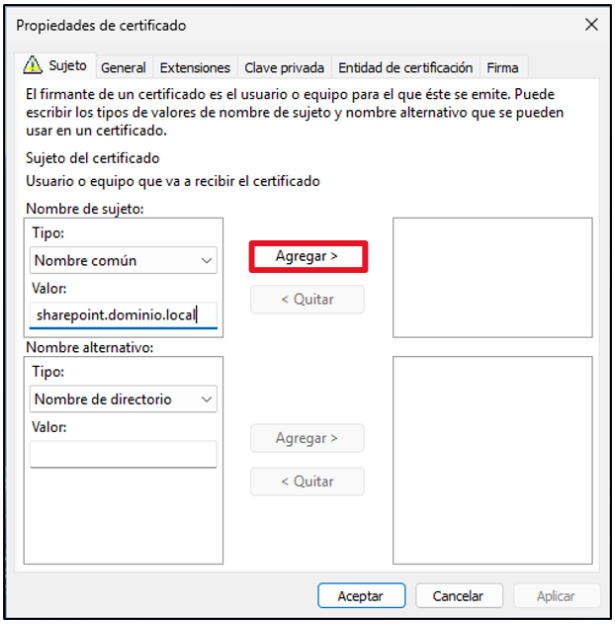
Una de las configuraciones adicionales a destacar en la configuración de Microsoft Sharepoint Server Subscription Edition es la configuración segura de los frontales expuestos a los administradores y clientes finales. Se considera una práctica recomendable en sitios web que alojarán datos susceptibles de ser comprometidos.

La utilización de protocolos y puertos seguros en la configuración de un servidor web garantizará la integridad y la confiabilidad de la comunicación. Con ello se mejorará la privacidad de la información estableciendo un canal cifrado durante el acceso a la información.

Paso	Descripción
1.	Acceder al servidor frontal de Sharepoint con un usuario con privilegios de administración.  *Ilustración 59 - Administración del servidor*
2.	Haga clic en “Herramientas”, y a continuación, “Powershell”.  *Ilustración 60 - Apertura de Powershell*

3.	Introduzca el comando “certlm.msc”, y pulse la tecla “Entrar”.  *Ilustración 61 - Apertura de consola de administración de certificados*
4.	En la consola de administración de certificados de máquina, haga clic con el botón derecho en “Personal”, y seleccione “Todas las tareas > Solicitar un nuevo certificado…”.  *Ilustración 62 - Solicitud de un nuevo certificado*
5.	En el asistente de instalación de certificados, pulse en “Siguiente”.  *Ilustración 63 - Asistente de configuración de certificados*

6.	Para continuar con las plantillas definidas en la entidad de certificación de Active Directory, haga clic en “Siguiente”.  *Ilustración 64 - Asistente de configuración de certificados*
7.	Seleccione la plantilla de certificados web deseada, en este caso “SSL”, y pulse sobre “Se necesita más información para inscribir este certificado. Haga clic para configurar los valores.”.  *Ilustración 65 - Selección de plantilla de certificados*

8.	En las propiedades del certificado, se hará clic sobre “DN completo” en la sección “Nombre de sujeto:”, y se seleccionará “Nombre común”.  *Ilustración 66 - Introducción de Nombre común*
9.	Introduzca el nombre del servicio de sharepoint que se expondrá al usuario final y pulse en “Agregar”.  *Ilustración 67 - Introducción de Nombre común*

10.	En caso de existir nombres alternativos, introdúzcalos del mismo modo, seleccionando en “Nombre alternativo” el parámetro “DNS”.
11.	Tras finalizar la configuración del certificado, introduzca un nombre descriptivo y pulse en “Aplicar” y “Aceptar”.

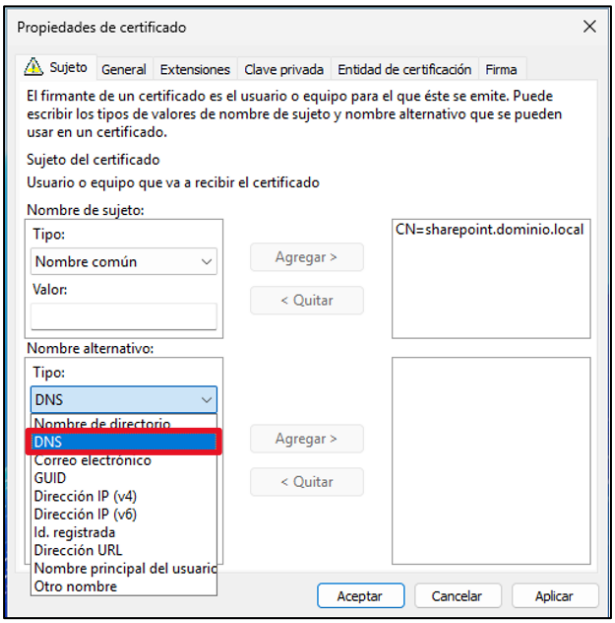


Ilustración 68 - Introducción de alias DNS alternativos

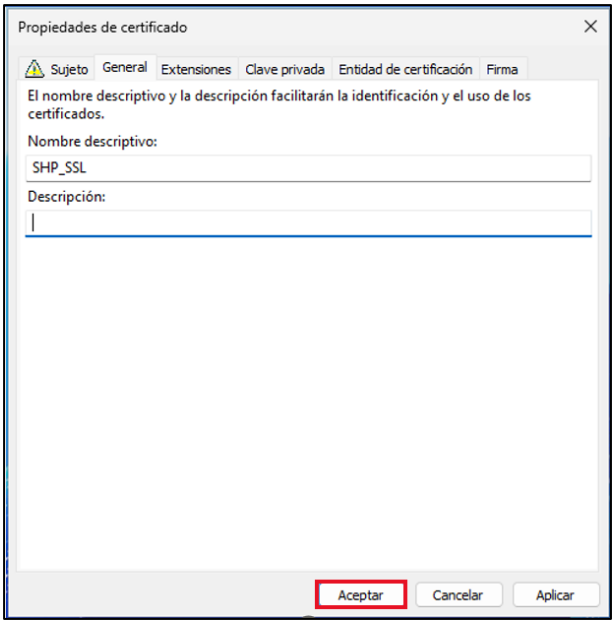
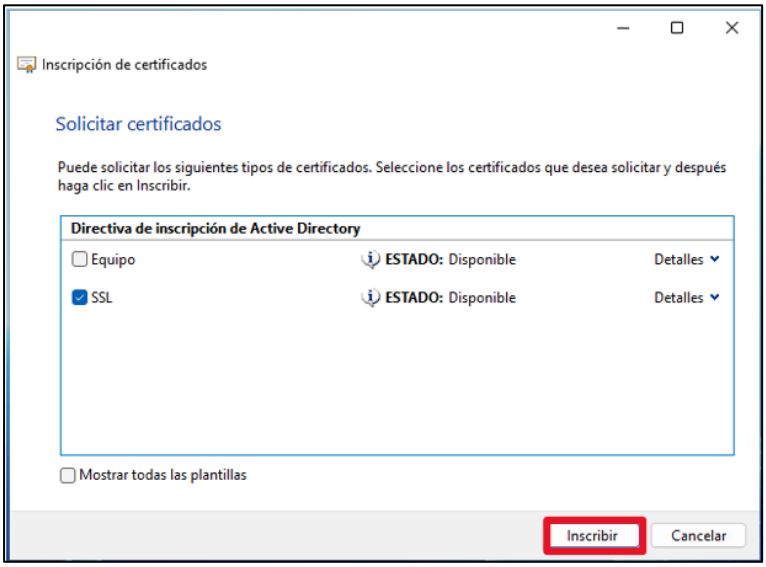
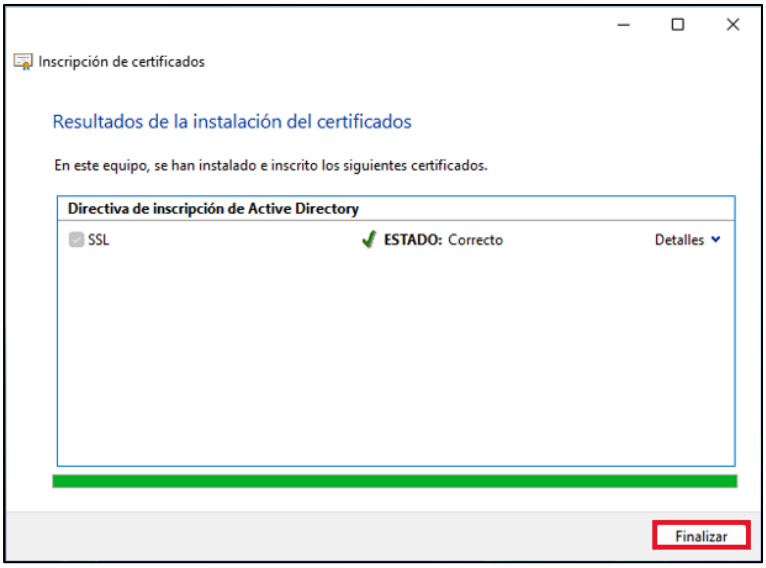
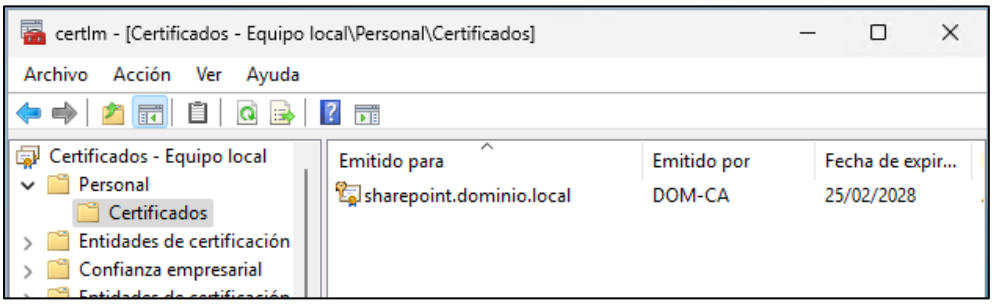
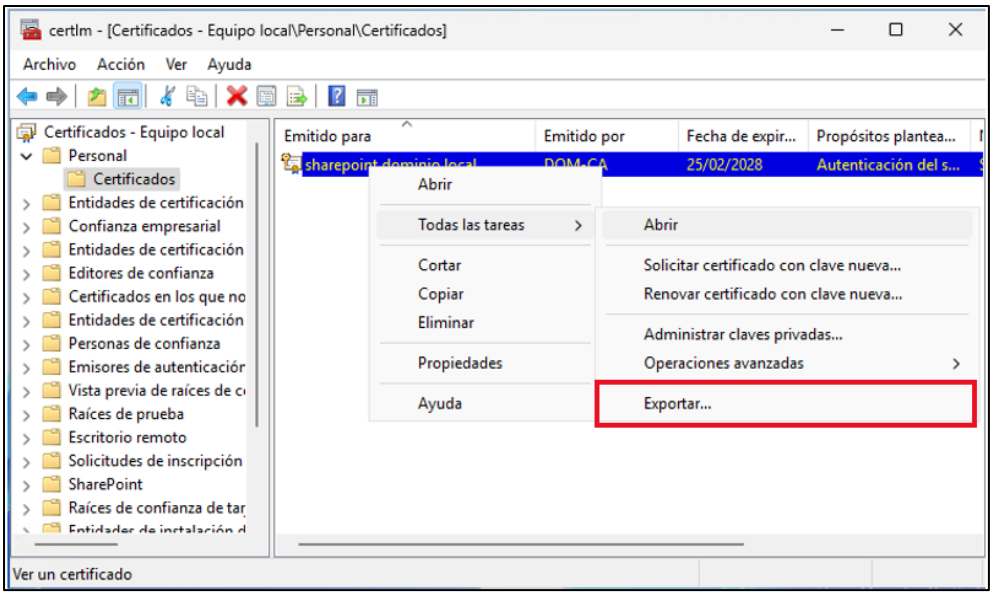
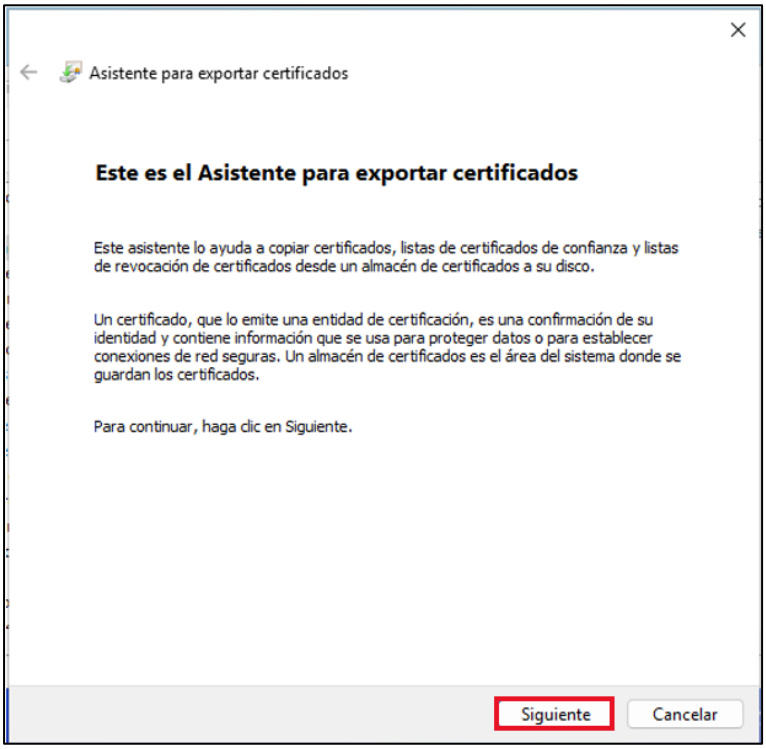
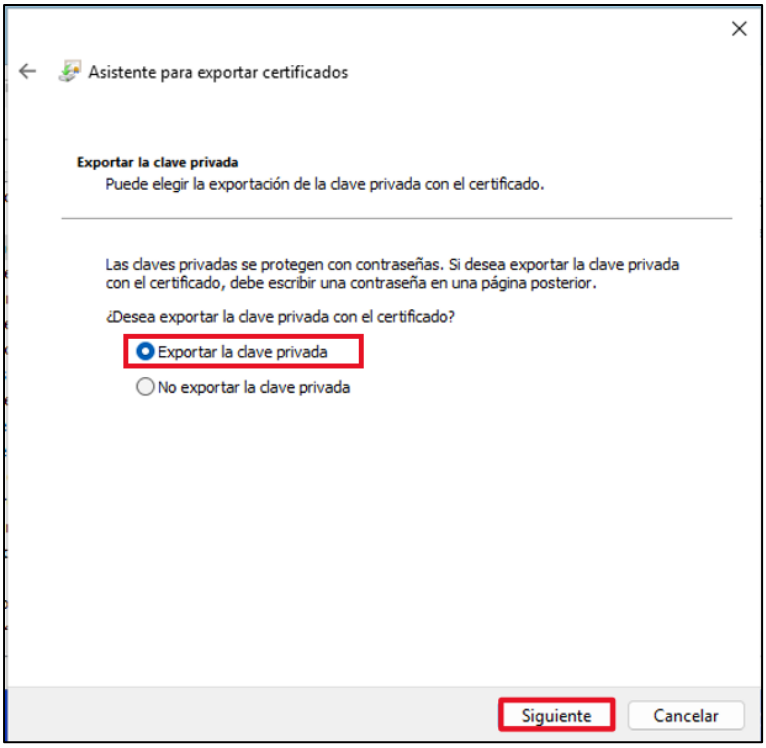


Ilustración 69 - Asistente de configuración de certificado

12.	A continuación, pulse en “Inscribir” para generar el certificado.  *Ilustración 70 - Asistente de creación de certificados*
13.	Pulse en el botón “Finalizar”.  *Ilustración 71 - Finalizar asistente de inscripción de certificados*

14.	A continuación, acceda a “Certificados – Equipo local > Personal > Certificados” y observe el nuevo certificado generado.  *Ilustración 72 - Certificados de máquina*
15.	Pulse con el botón derecho sobre éste, y diríjase a “Todas las tareas > Exportar”.  *Ilustración 73 - Exportar certificado*

16.	Para comenzar con la copia del certificado, pulse en “Siguiente”.  *Ilustración 74 - Asistente para exportar certificados*
17.	Seleccione “Exportar la clave privada” y haga clic en “Siguiente”.  *Ilustración 75 - Exportar clave privada*

18.	De nuevo, pulse en “Siguiente”.

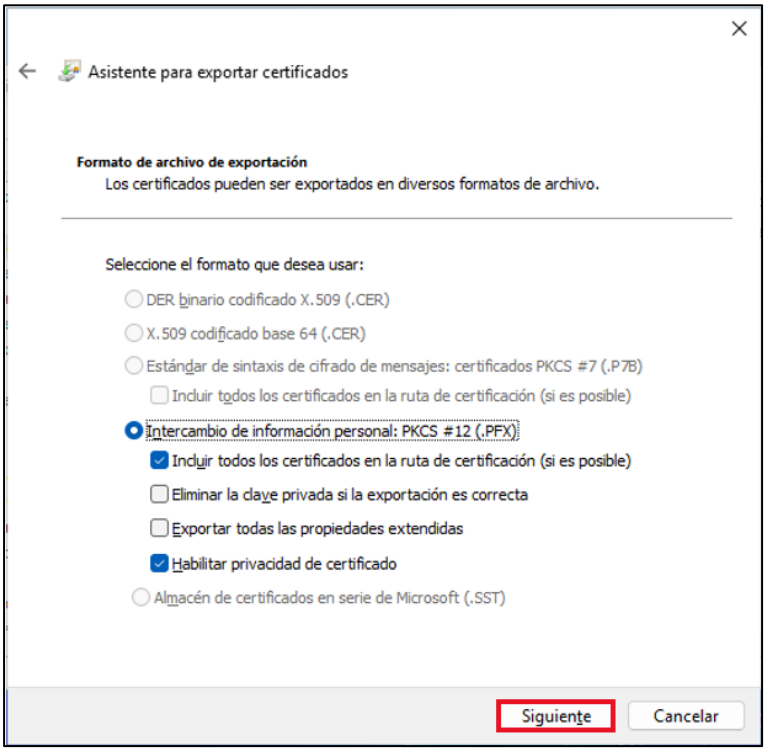


Ilustración 76 - Formato de exportación de certificados

19.	Establezca una contraseña segura para el certificado, y pulse en “Siguiente”.

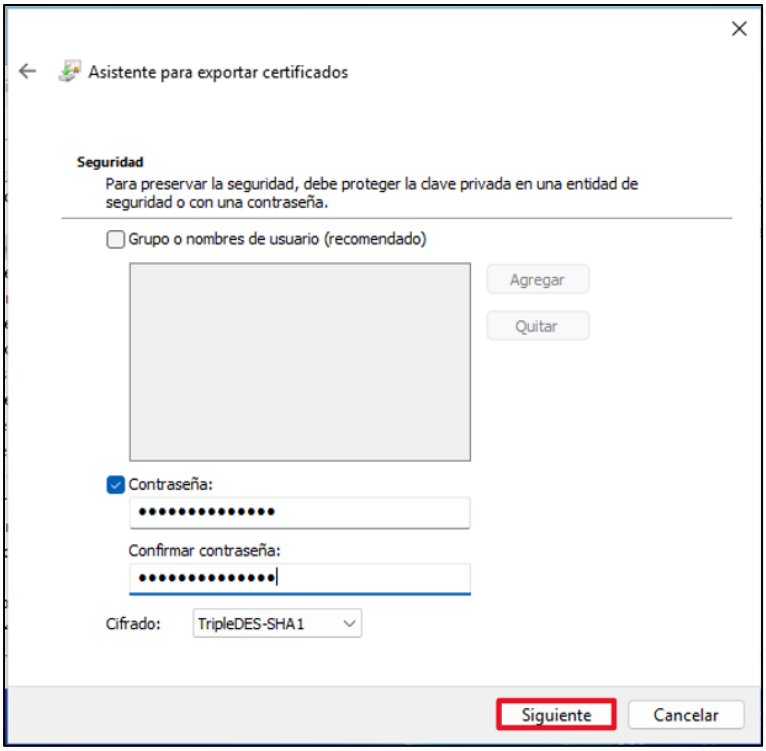
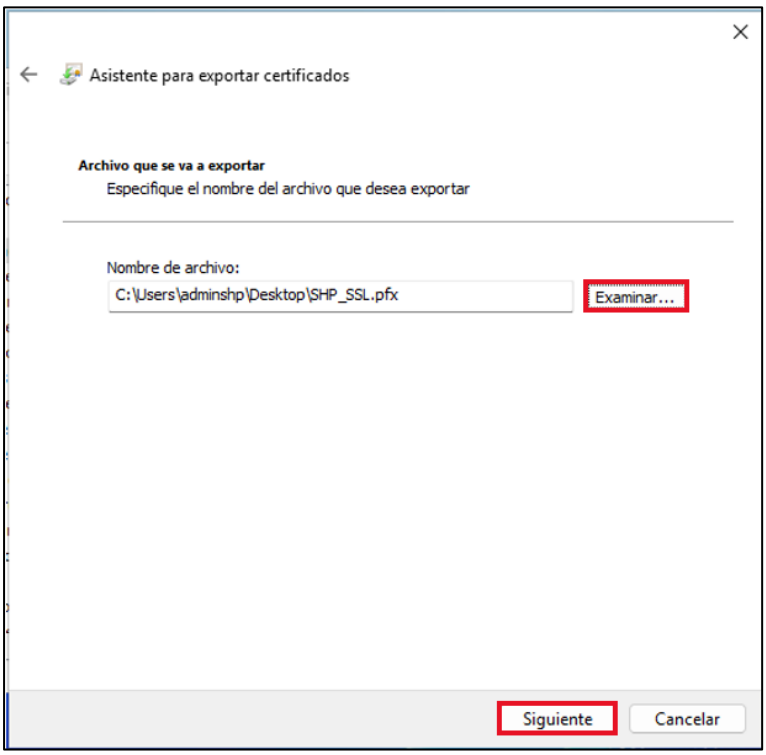
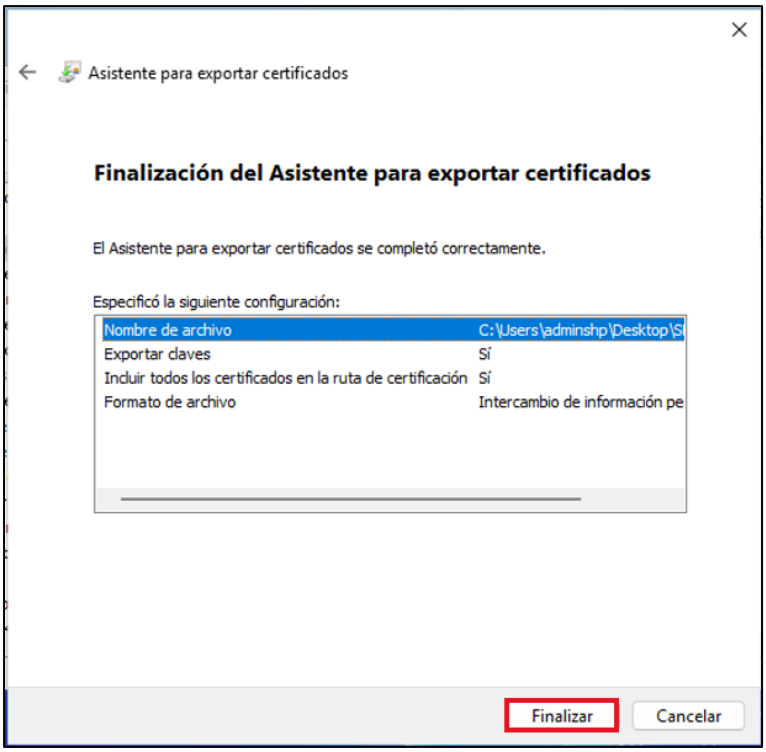
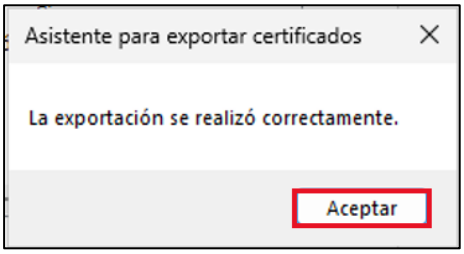
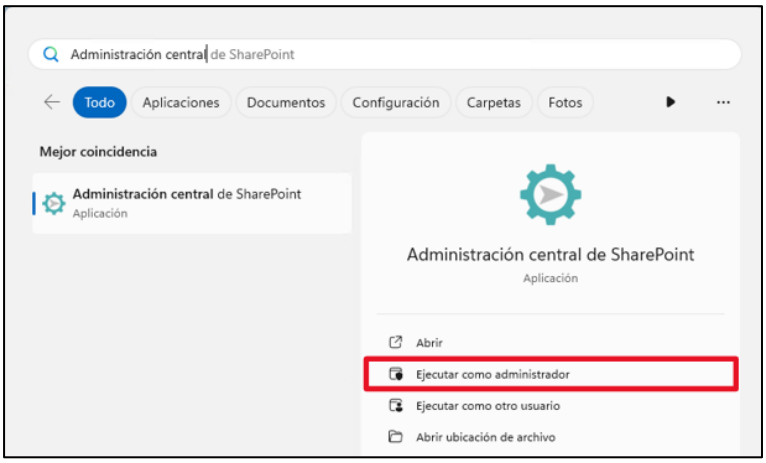
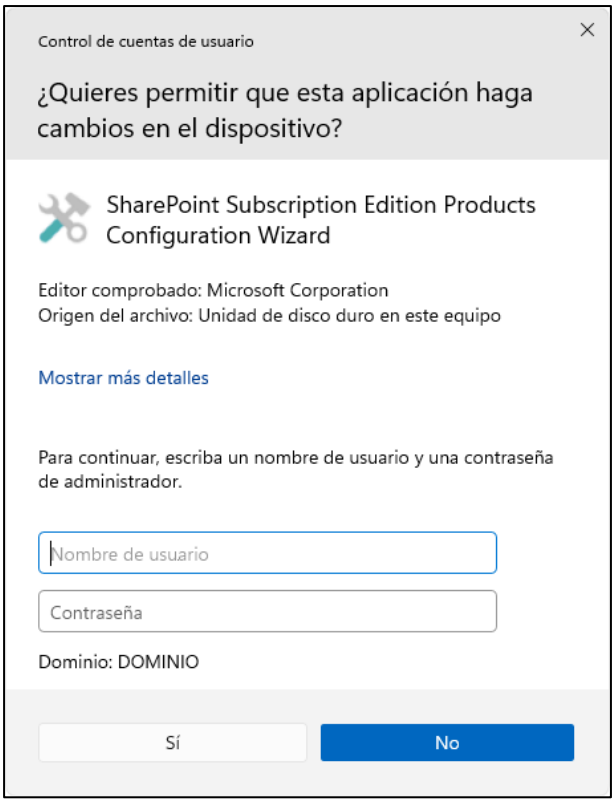
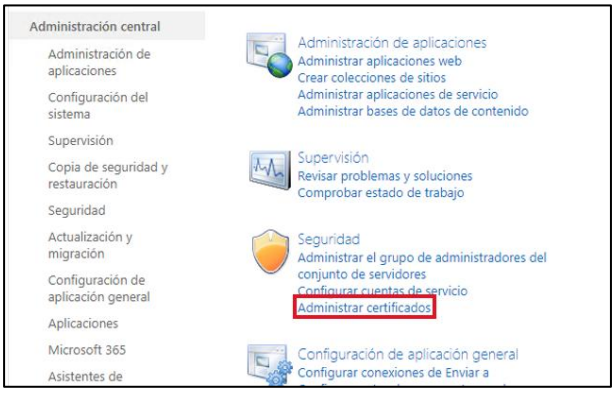
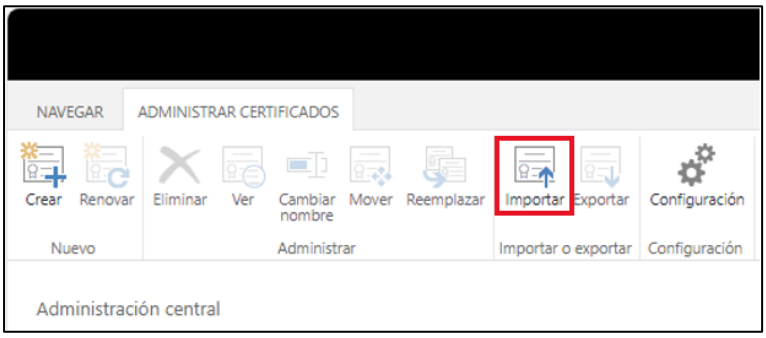
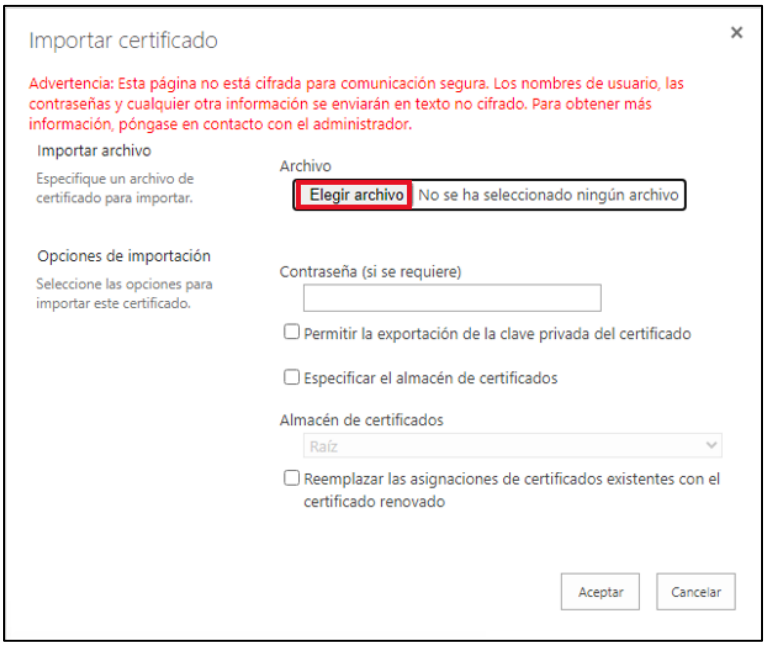


Ilustración 77 - Introducción de contraseña

20.	Seleccione la ruta y nombre donde desee guardar el archivo "*.pfx" pulsando sobre el botón "Examinar" y posteriormente, haga clic en "Siguiente".  *Ilustración 78 - Asistente para exportar certificados*
21.	Pulse "Finalizar" para cerrar el asistente de exportación de certificados.  *Ilustración 79 - Finalizar asistente para exportar certificados*

22.	Haga clic en “Aceptar”.  *Ilustración 80 - Finalizar asistente para exportar certificados* **Nota**: En caso de que su organización disponga de un departamento de certificación o exista una entidad pública que gestione los certificados, deberá omitir estos pasos y realizar una solicitud de certificado web siguiendo los procedimientos oficiales de su compañía.
23.	Tras la exportación del certificado, acceda a la consola de “Administración central de SharePoint” como administrador.  *Ilustración 81 - Apertura de Administración central de Sharepoint*

24.	Introduzca un usuario y contraseña con privilegios de administración en el servidor Sharepoint.  *Ilustración 82 - Acceso a consola de administración central* **Nota:** En caso de solicitar una nueva autenticación NTLM, introduzca un usuario y contraseña con privilegios de administración de la consola de Sharepoint.
	Haga clic en “Administrar certificados” ubicado en la sección de “Seguridad”.  *Ilustración 83 - Acceso a la administración de certificados*

25.	Pulse sobre el botón “Importar”.  *Ilustración 84 - Importar certificados*
26.	Haga clic en “Elegir archivo”.  *Ilustración 85 - Importar certificados*

27.	Diríjase a la carpeta donde se ha almacenado el certificado, selecciónelo y pulse “Abrir”.

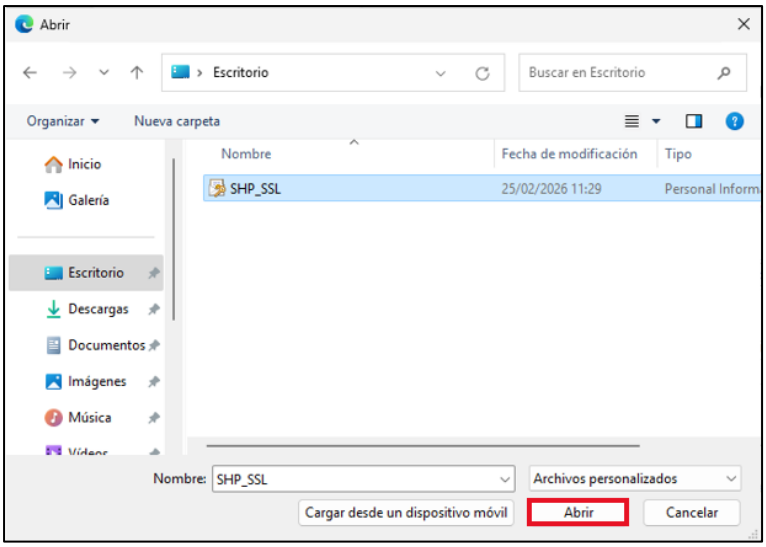


Ilustración 86 - Selección de certificado

28.	Introduzca la contraseña y pulse en “Aceptar”.

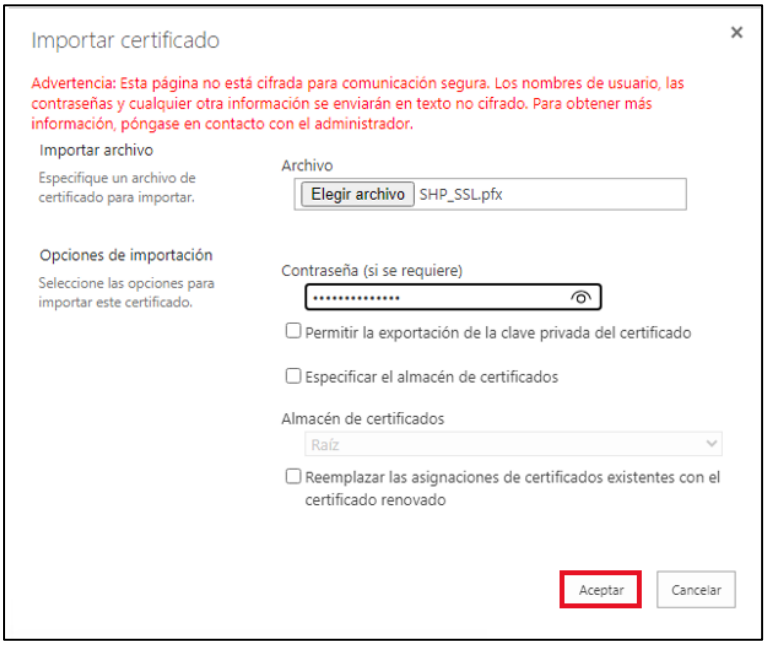
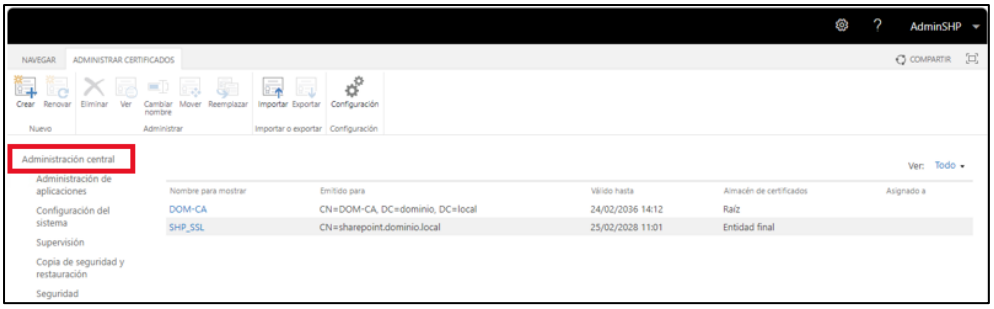
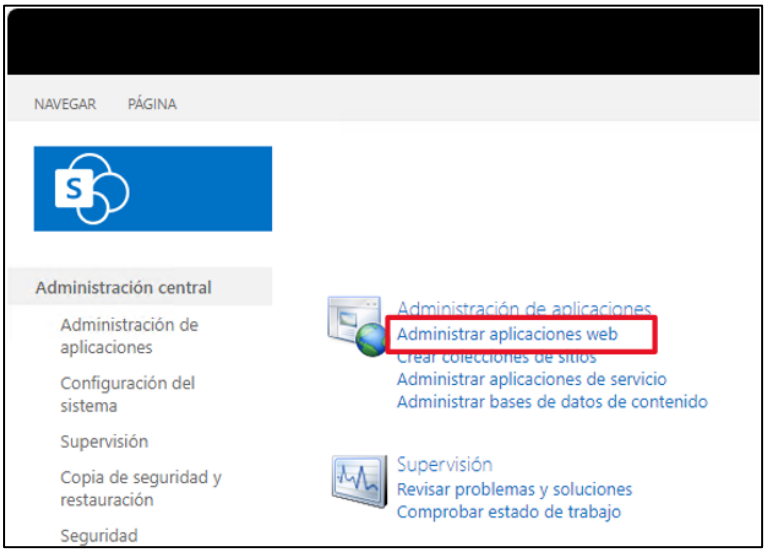
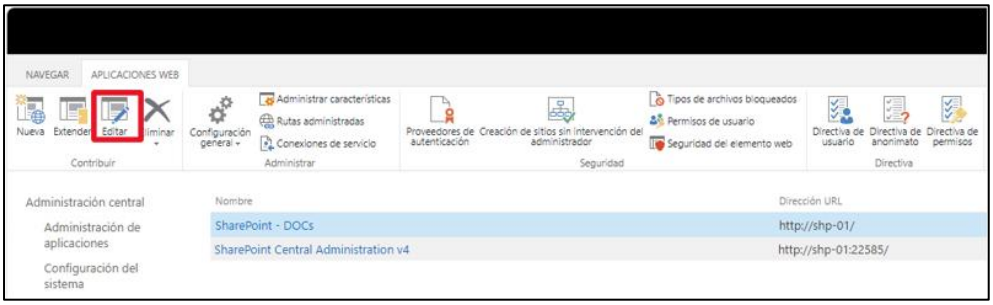
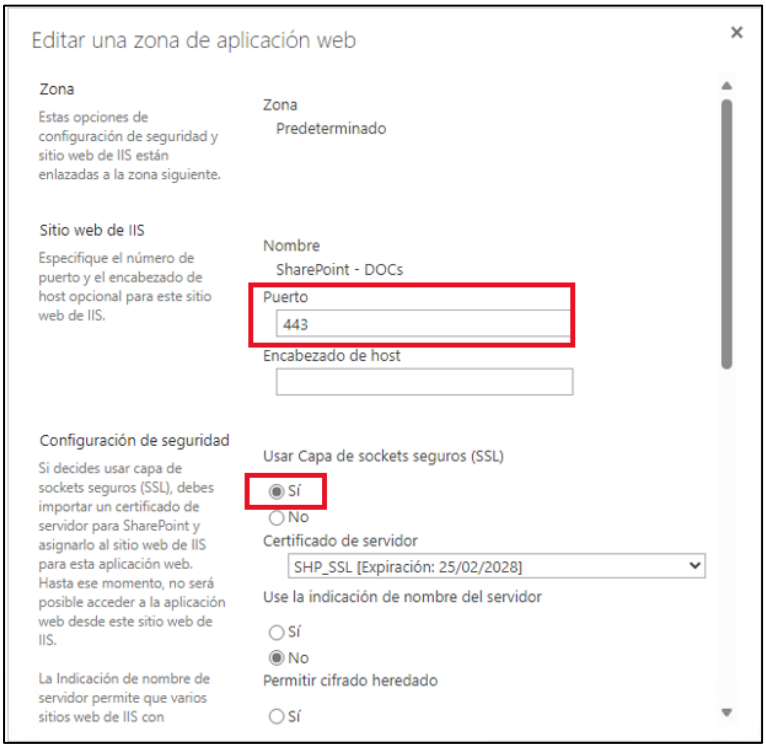


Ilustración 87 - Finalizar asistente de importación de certificados en Sharepoint

29.	La herramienta mostrará los certificados Raíz, Entidad subordinada (si existiese) y Entidad final recogidos en el fichero *.pfx. Pulsar en “Aceptar”.  *Ilustración 88 - Previsualización de certificado*
30.	El certificado quedará importado en Sharepoint. Para continuar, pulse sobre “Administración central”.  *Ilustración 89 - Consola de administración central*
31.	En la sección “Administración de aplicaciones”, seleccione “Administrar aplicaciones web”.  *Ilustración 90 - Acceso a la administración de aplicaciones*

32.	Hacer clic sobre la aplicación deseada, y a continuación, pulsar en “Editar”.  *Ilustración 91 - Edición de aplicación web*
33.	Seleccione la zona de exposición del sitio de Sharepoint. En este caso, “Predeterminado”.  *Ilustración 92 - Acceso a zona predeterminada*
34.	A continuación, haga clic en “Sí” en la sección de “Configuración de seguridad > Usar Capa de sockets seguros (SSL)” y seleccione el certificado en el menú desplegable. A su vez, introduzca el puerto “443” en sustitución del puerto 80 existente.  *Ilustración 93 - Configuración de certificado*

35.	Diríjase hasta el final del asistente e introduzca la dirección URL correspondiente. A continuación, pulse en “Guardar”.

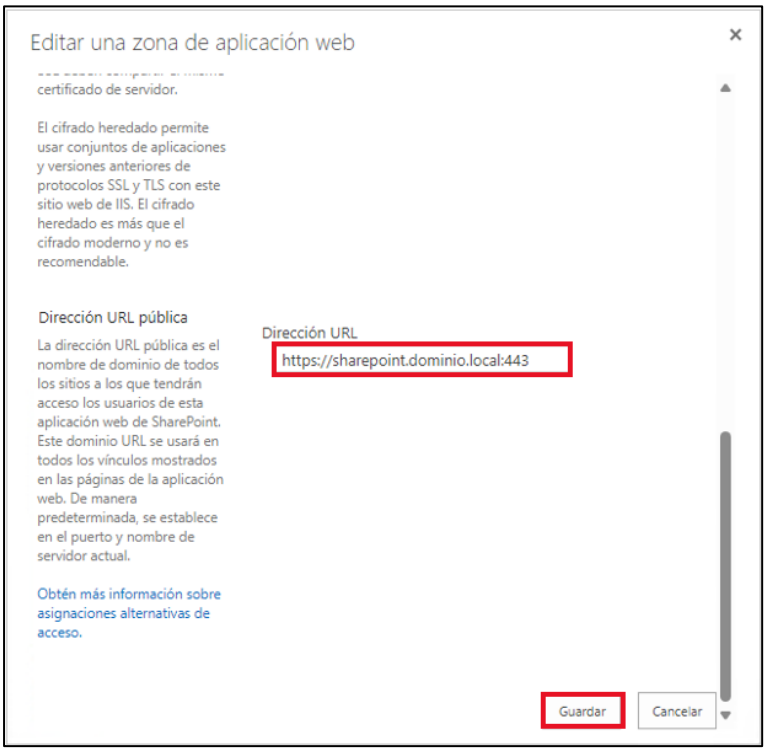
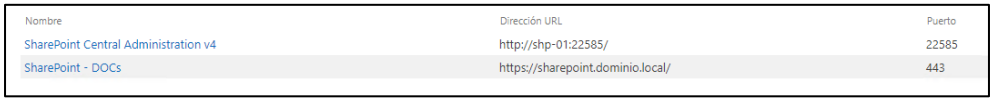


Ilustración 94 - Configuración de URL de acceso

Nota: La URL indicada deberá coincidir con el nombre común establecido en el certificado generado al inicio de este procedimiento.

36.	A continuación, observará como la configuración de la aplicación web ha cambiado.



Nombre	Dirección URL	Puerto
SharePoint Central Administration v4	http://shp-01:22585/	22585
SharePoint - DOCs	https://sharepoint.dominio.local/	443

Ilustración 95 - Configuración de HTTPS y puerto para acceder a la aplicación web

37. Realice la misma configuración para la consola de Administración Central de Sharepoint.

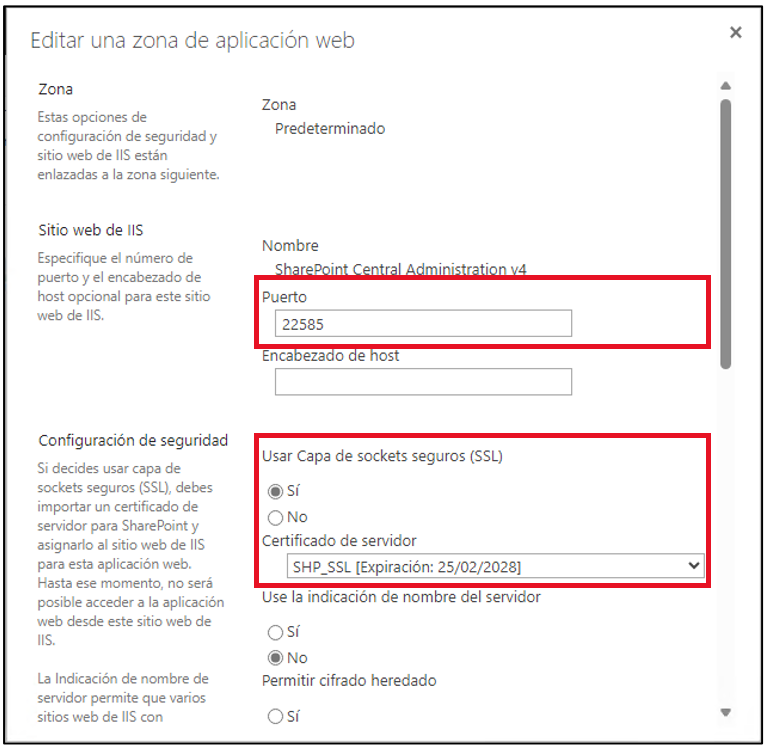
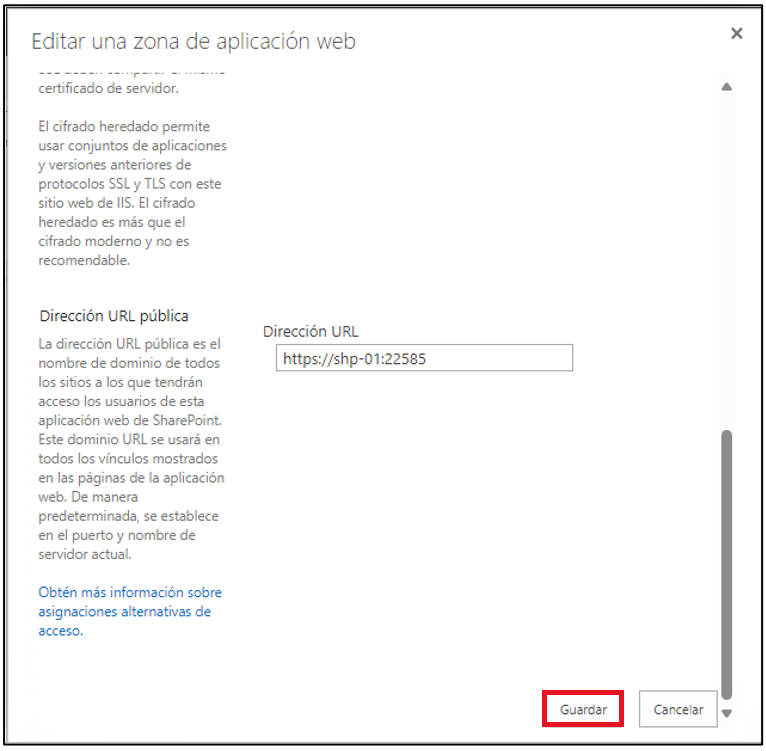
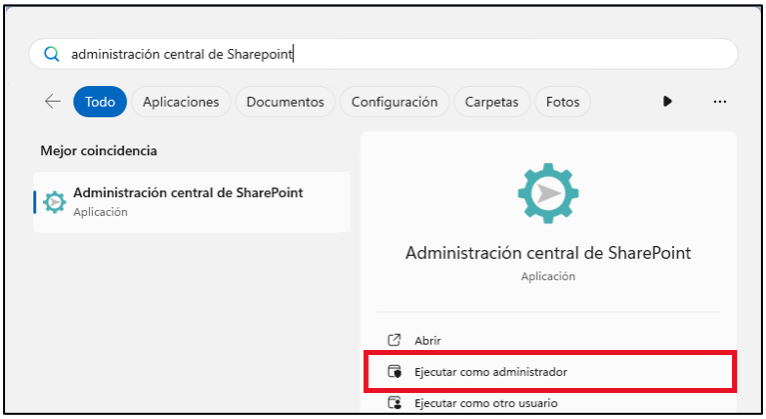
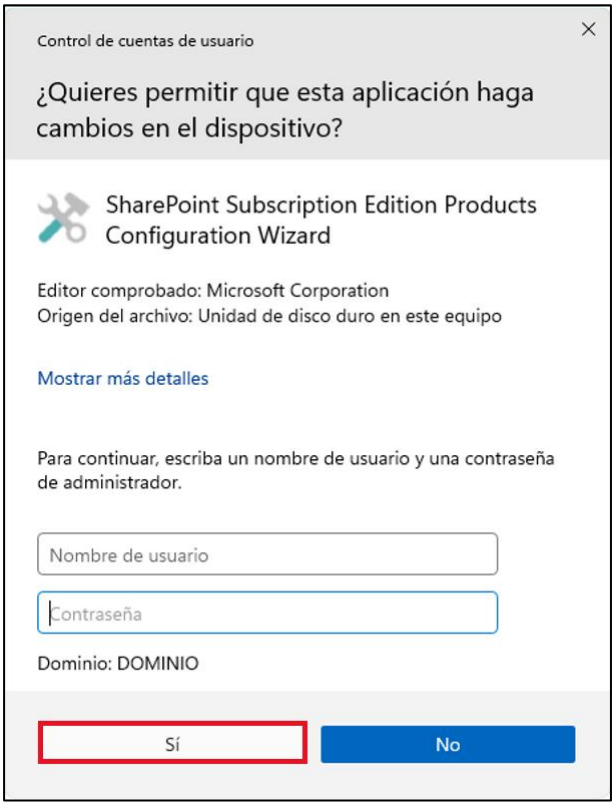
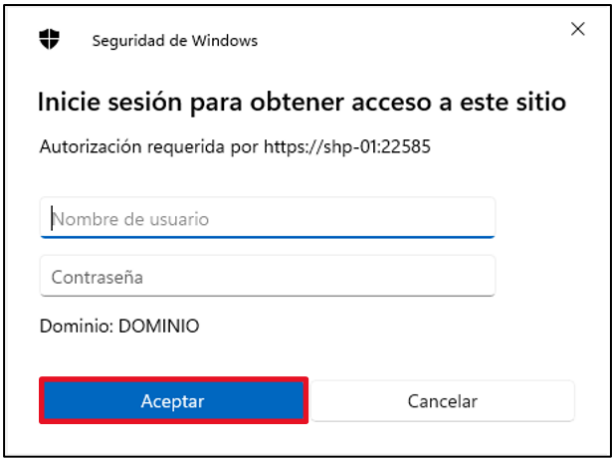


Ilustración 96 - Configuración SSL

Nota: En este caso, asegúrese de no modificar el puerto de administración.

38.	Pulse en Guardar para hacer efectivo el cambio.  *Ilustración 97 - Configuración de URL de administración* **Nota**: Tras la realización de este cambio, la consola de administración quedará inaccesible mediante protocolos y puertos inseguros (HTTP – 80), por lo que se deberá cerrar el navegador y acceder de nuevo mediante el icono de administración de Sharepoint.
39.	Busque de nuevo la consola de “Administración central de SharePoint” y ejecútela como administrador.  *Ilustración 98 - Ejecución de consola de administración*

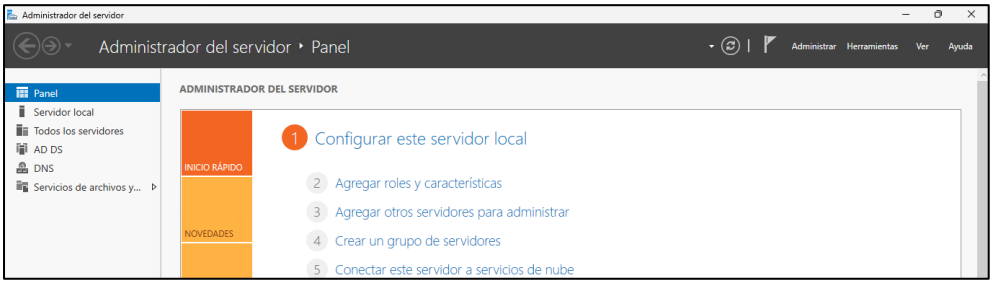
40.	Introduzca un usuario con privilegios administrativos en el servidor.  *Ilustración 99 - Acceso a consola de Administración central*
41.	Introduzca las credenciales de administración de Sharepoint y pulse “Aceptar”.  *Ilustración 100 - Acceso a consola de administración central*
42.	Como podrá observar, la consola de administración y aplicaciones web tan solo estarán accesibles mediante el uso de un certificado web, que proporcionará un blindaje adicional, garantizando la confidencialidad, integridad y autenticidad de las comunicaciones.

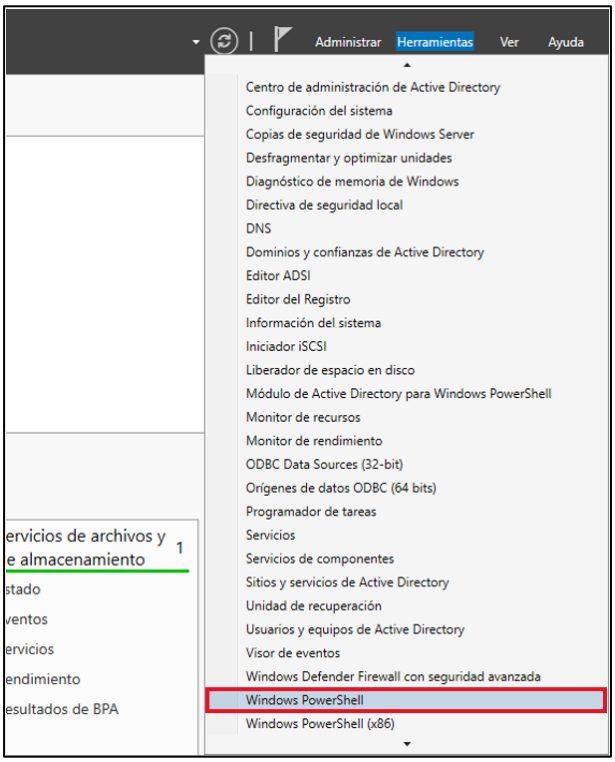
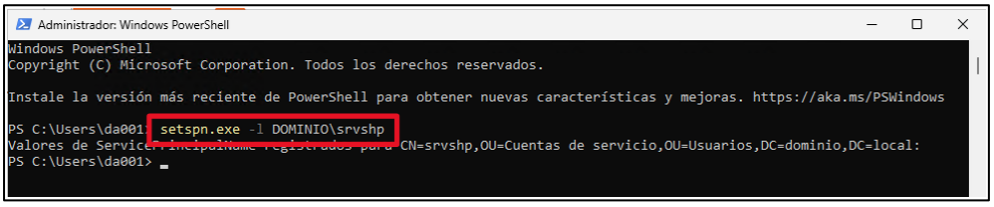
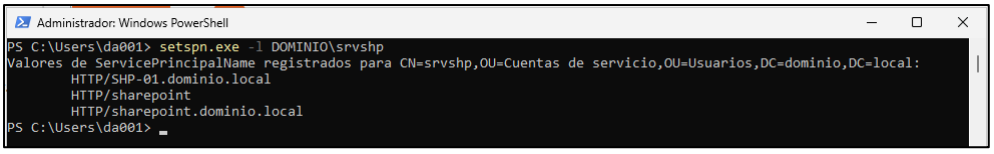
ANEXO A.2.2. Mecanismos de autenticación

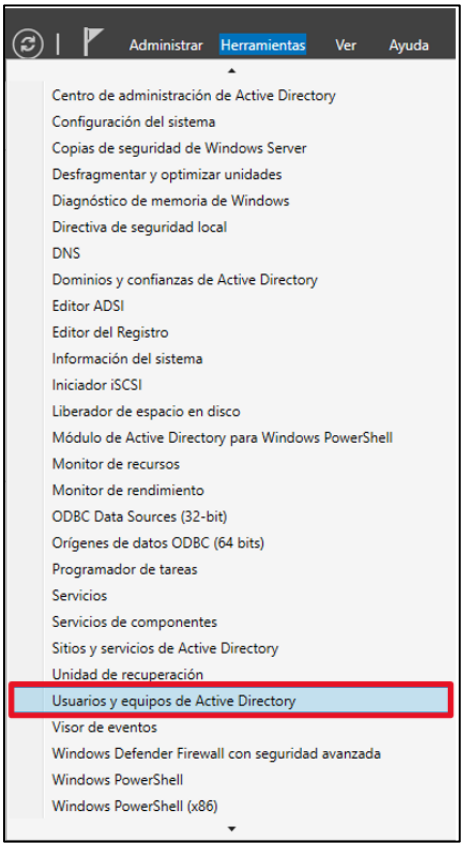
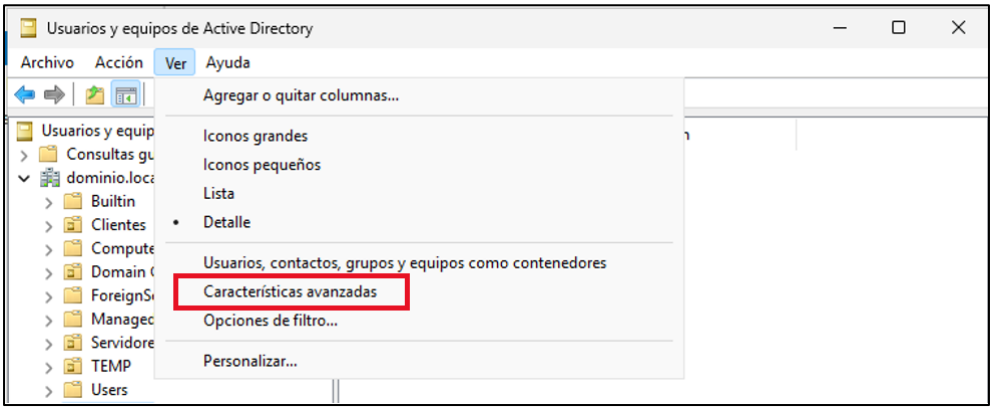
El protocolo NTLM se considera actualmente un mecanismo de autenticación obsoleto y vulnerable, debido a no soportar métodos modernos de cifrado. Por ello, para evitar comprometer la integridad de las credenciales dentro del entorno de red es recomendable la transición hacia mecanismos como Kerberos o esquemas de federación de identidades (como SAML u OpenID Connect).

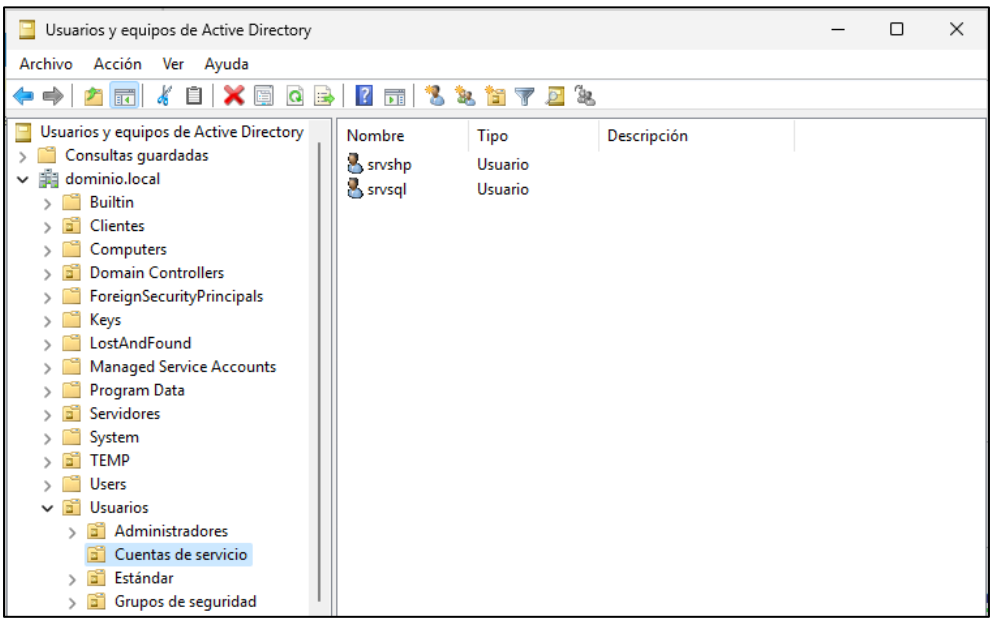
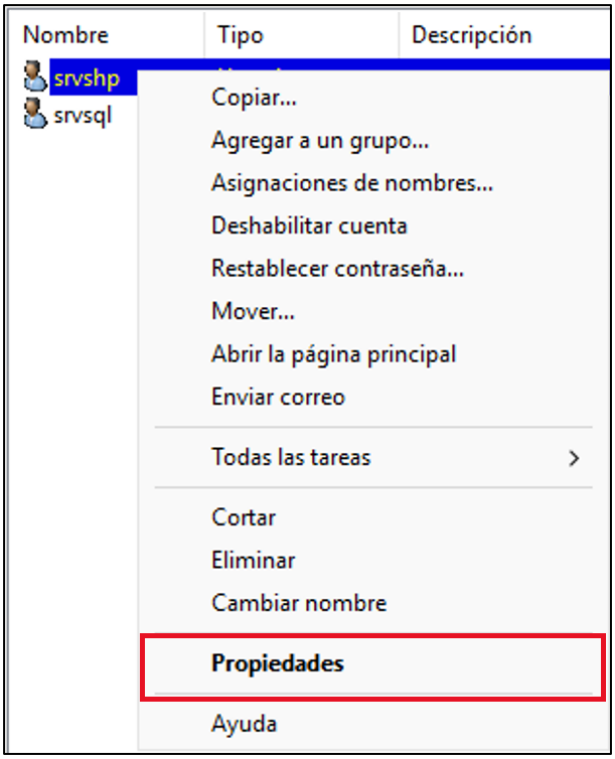
Estas alternativas ofrecen un modelo robusto de seguridad basado en tickets y proveedores de identidad centralizados, permitiendo una validación bidireccional, el uso de cifrado fuerte y la integración de factores de autenticación multifactor (MFA). Adoptar estos estándares no solo mitiga los riesgos críticos asociados a NTLM, sino que garantiza el cumplimiento de los marcos de seguridad modernos y mejora la interoperabilidad en entornos On premise, en la nube o híbridos.

A continuación, se mostrará la configuración básica de Kerberos para una aplicación web de Sharepoint Subscription Edition.

Paso	Descripción
1.	Acceda a un controlador de dominio del entorno con un usuario con privilegios de administración del dominio.  *Ilustración 101 - Administración del controlador de dominio*

2.	Haga clic en “Herramientas” y posteriormente, “Powershell”.  *Ilustración 102 - Acceder a la consola de Windows Powershell*
3.	Confirme que la cuenta de servicio utilizada durante la instalación de Sharepoint no dispone de registros “SPN” configurados que puedan provocar duplicidad alguna, mediante la ejecución del comando: *setspn.exe -l DOMINIO\srvshp*  *Ilustración 103 - Ejecución del comando*
4.	Ejecute los siguientes commandos para la creación de los SPN asociados al servicio de Sharepoint: *setspn.exe -S HTTP/sharepoint.dominio.local DOMINIO\srvshp* *setspn.exe -S HTTP/sharepoint DOMINIO\srvshp* *setspn.exe -S HTTP/SHP-01.dominio.local DOMINIO\srvshp*  *Ilustración 104 - Comprobación de entradas SPN asociadas a la cuenta de servicio*

5.	Acceda a la consola de administración de usuarios y equipos de directorio activo haciendo clic en "Herramientas > Usuarios y equipos de Active Directory" en la consola de "Server Manager".  *Ilustración 105 - Acceso a la consola de administración de usuarios*
6.	Asegúrese que la visualización de las características avanzadas está habilitada en el menú "Ver".  *Ilustración 106 - Habilitar "Características avanzadas"* **Nota**: En caso de no estar habilitada, pulse sobre ella para configurarla

7.	Diríjase a la unidad organizativa donde se encuentra la cuenta de servicio utilizada por Sharepoint.  *Ilustración 107 - Unidad organizativa contenedora de las cuentas de servicio*
8.	Haga clic derecho sobre la cuenta de servicio, y a continuación, seleccione “Propiedades”.  *Ilustración 108 - Propiedades de la cuenta de servicio*

9.	Diríjase a la pestaña “Delegación”.

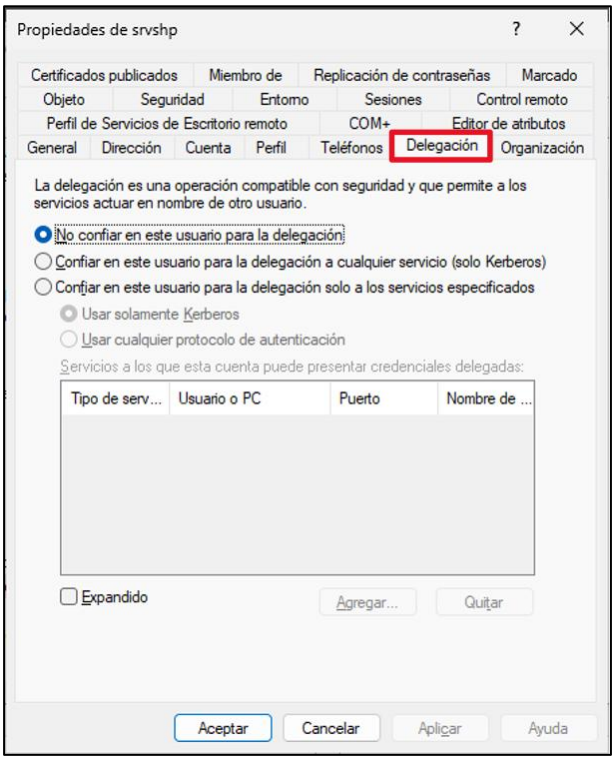
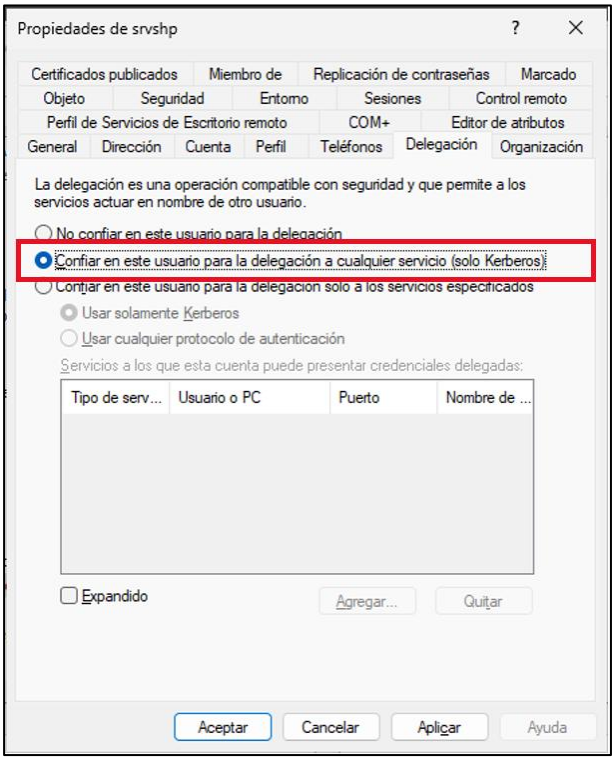
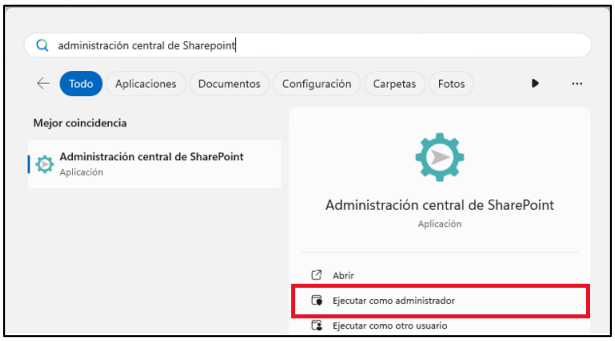
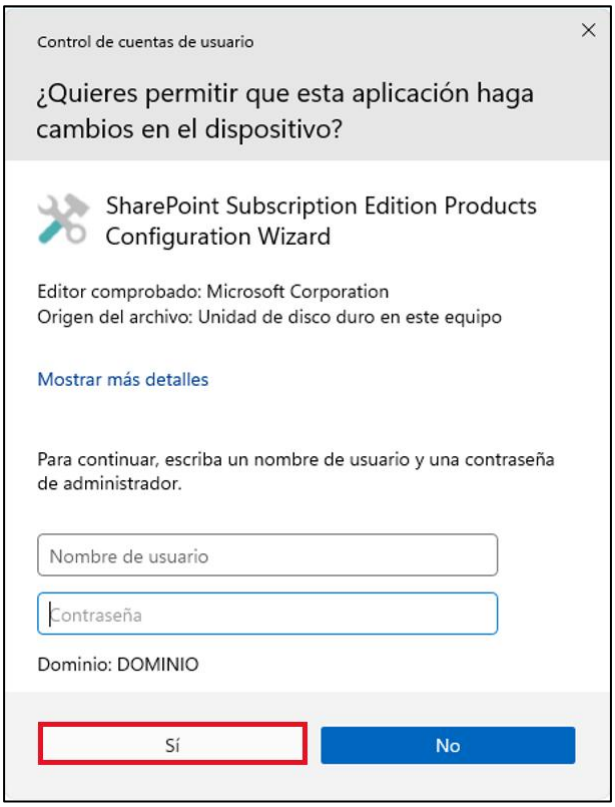
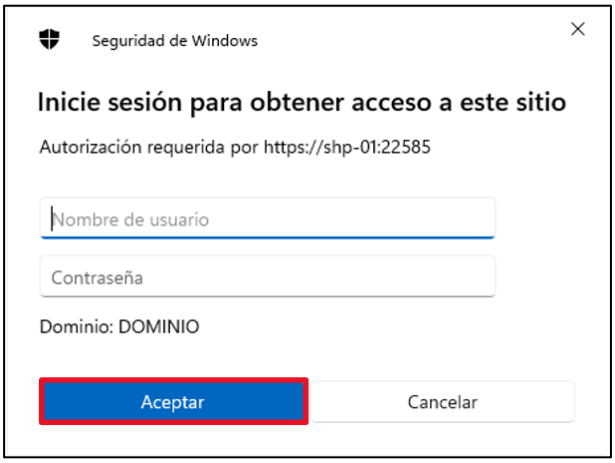
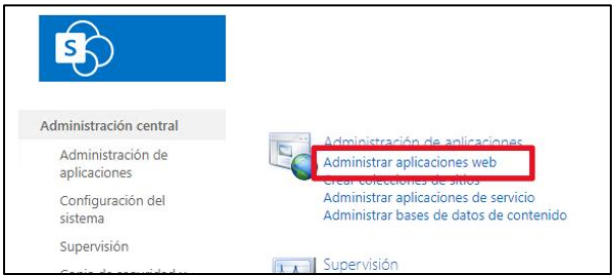
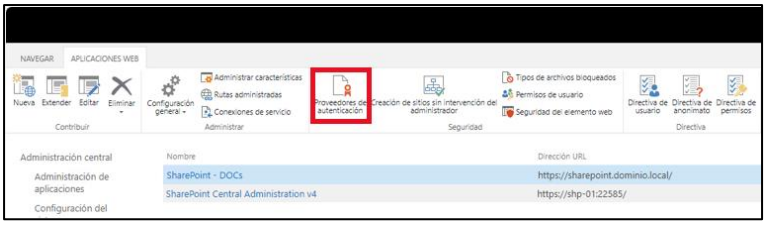
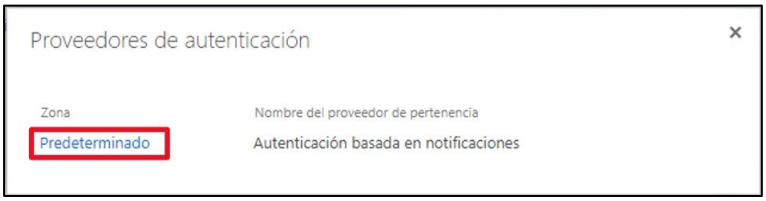


Ilustración 109 - Pestaña "Delegación"

10.	Configure la delegación para “Confiar en este usuario para la delegación a cualquier servicio (solo Kerberos)”. A continuación, pulse en “Aplicar” y “Aceptar”.  *Ilustración 110 - Configuración de la delegación Kerberos* **Nota**: En entornos controlados se podrá seleccionar “Confiar en este usuario para la delegación solo a los servicios especificados”, y agregar los servicios para los que se desee confiar la delegación.
11.	Una vez concedidos los permisos, acceda a la consola de “Administración central de SharePoint” y ejecútela como administrador.  *Ilustración 111 - Acceso a la consola de Administración central de Sharepoint*

12.	Introduzca un usuario con privilegios administrativos en el servidor.  *Ilustración 112 - Acceso a la consola de Administración central de Sharepoint*
13.	Introduzca las credenciales de administración de Sharepoint y pulse “Aceptar”.  *Ilustración 113 - Acceso a la consola de Administración central de Sharepoint*

14.	Acceda a “Administrar aplicaciones web” en la sección de “Administración de aplicaciones”.  *Ilustración 114 - Acceso a administración de aplicaciones web*
15.	Seleccione la aplicación web en la que desea implementar Kerberos como mecanismo de autenticación y a continuación, pulse en “Proveedores de autenticación”.  *Ilustración 115 - Configuración de Proveedores de autenticación*
16.	Seleccione la zona donde se encuentra la aplicación web. En este caso, “Predeterminado”.  *Ilustración 116 - Acceso a la configuración de la aplicación web*

17.	En primer lugar, es imperativo confirmar que el "Acceso anónimo" se encuentra deshabilitado. Permitir la autenticación anónima en las aplicaciones web anulará la eficacia del control de autenticación. Así mismo, las actividades realizadas en una sesión anónima carecerán de trazabilidad al no poder ser vinculada con una cuenta específica. Asegúrese que dicha configuración no se encuentra marcada.

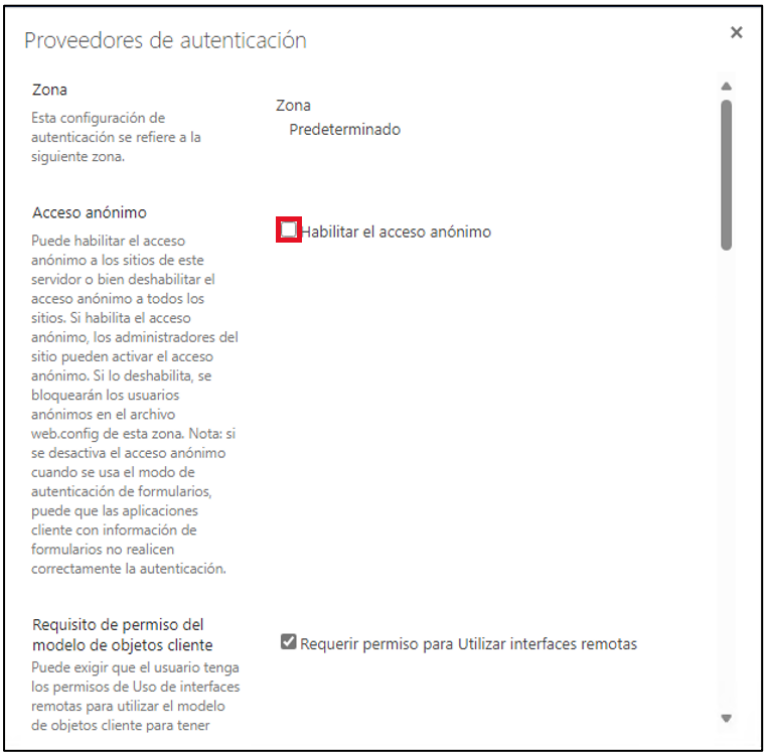


Ilustración 117 - Deshabilitar el acceso anónimo

18.	Desplace el menú de configuración hasta la sección de “Tipos de autenticación de notificaciones”, y en el menú desplegable “Autenticación de Windows integrada”, seleccione “Negociar (Kerberos)”.

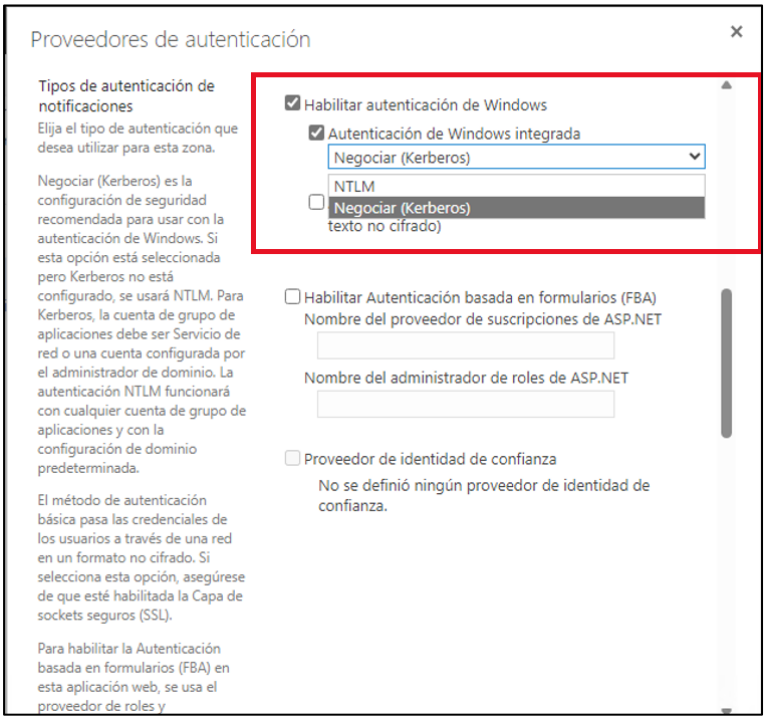


Ilustración 118 - Configuración de Kerberos como método de autenticación

19.	Diríjase hasta el final del asistente y pulse en “Guardar”.

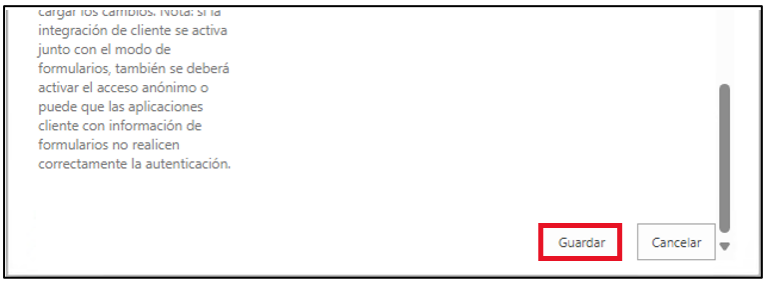
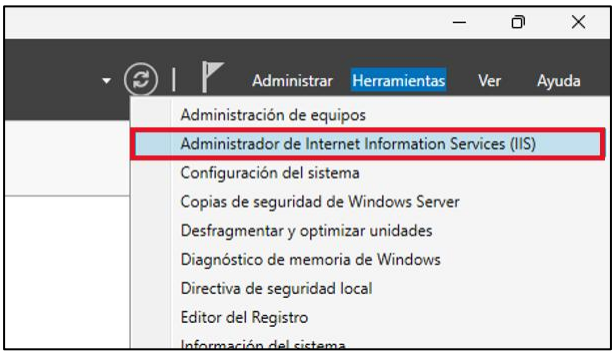
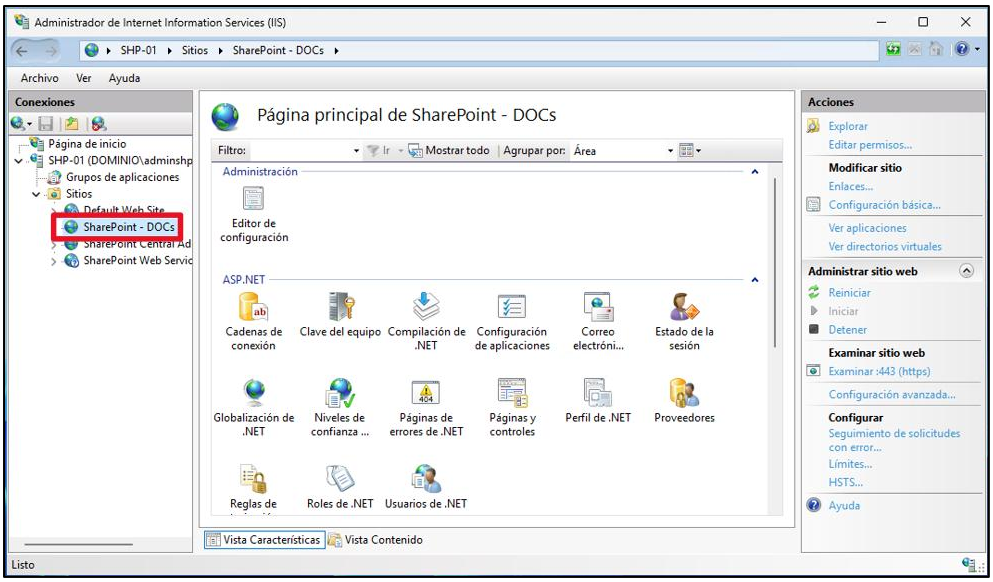


Ilustración 119 - Finalizar la configuración de autenticación

20.	A continuación, pulse en el botón de cerrar y finalice la configuración.

Ilustración 120 - Cerrar el menú de configuración

21.	Para continuar, en la administración del servidor (Server Manager), haga clic en “Herramientas” y “Administrador de Internet Information Services (IIS)”.  *Ilustración 121 - Acceso a la consola de Administración de IIS*
22.	Despliegue el servidor IIS configurado, y haga clic en la aplicación web que acaba de configurar. En este caso “Servidor – Sitios – Sharepoint – DOCs”.  *Ilustración 122 - Selección de Web Application*

23.	Busque en la sección IIS la herramienta de “Autenticación” y haga doble clic sobre ella.

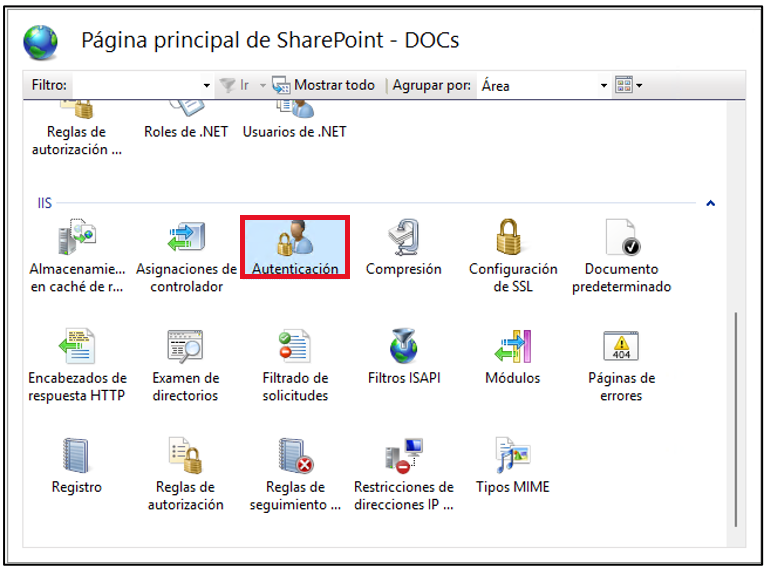


Ilustración 123 - Configuración de Autenticación

24.	Haga clic con el botón derecho sobre “Autenticación de Windows” y seleccione “Proveedores”.

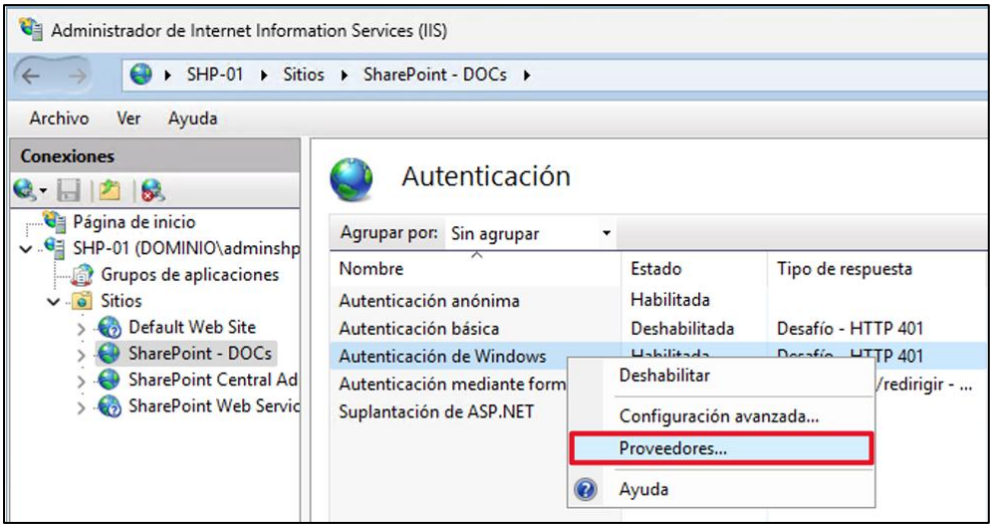
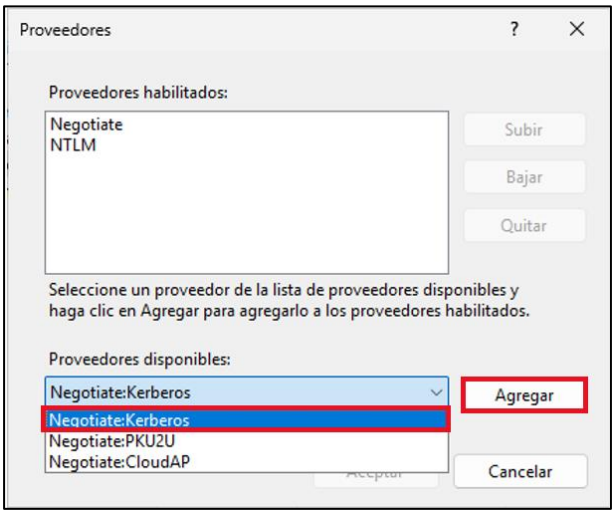
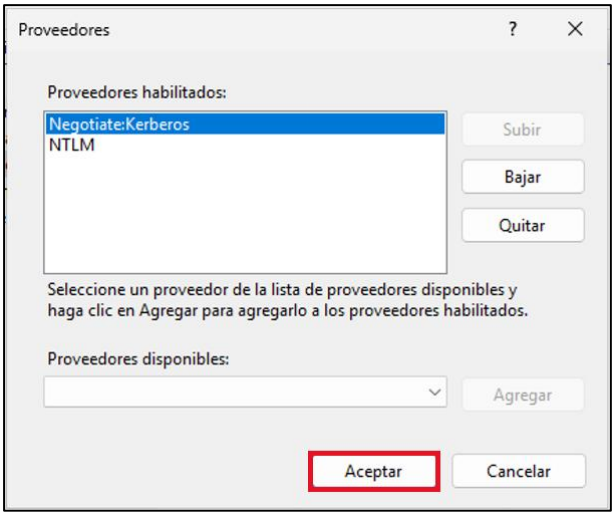
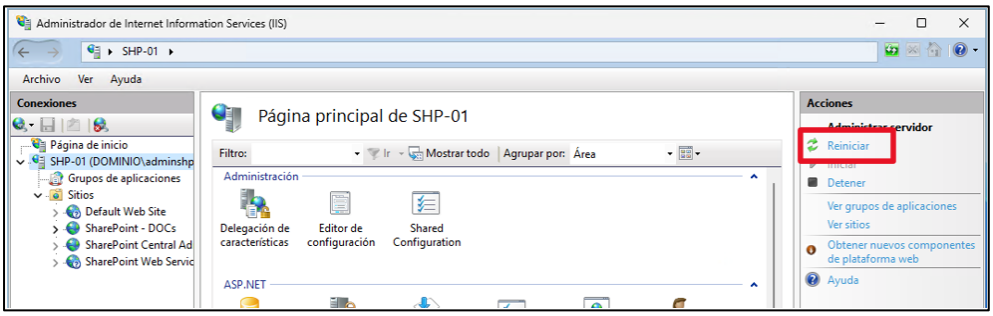
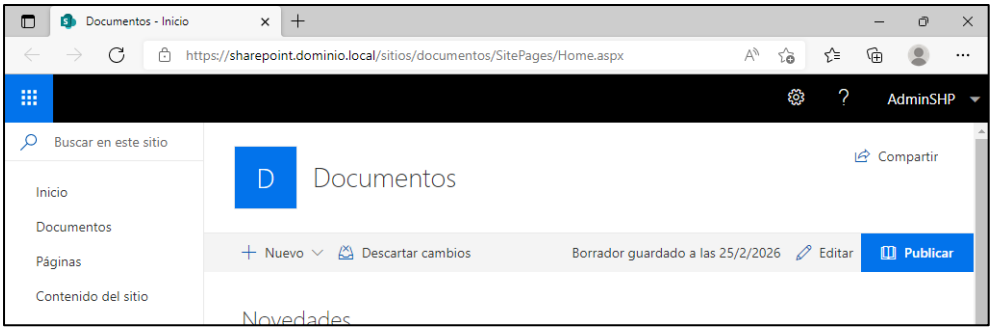


Ilustración 124 - Configuración de proveedores de autenticación

25.	En el menú desplegable “Proveedores disponibles”, seleccione “Negotiate (Kerberos)” y pulse sobre “Agregar”.  *Ilustración 125 - Configuración Kerberos IIS*
26.	Establezca la siguiente prioridad en los proveedores de autenticación mediante los botones “Subir”, “Bajar” y “Quitar” y a continuación, pulse en “Aceptar”.  *Ilustración 126 - Configuración Kerberos en IIS*

27.	Seleccione el nombre del servidor IIS y pulse en “Reiniciar” en el menú de Acciones.  *Ilustración 127 - Reinicio de servicio IIS*
28.	A continuación, si accede a la aplicación web con un usuario de Windows con permisos de lectura, el navegador iniciará sesión automáticamente (SSO).  *Ilustración 128 - Acceso a aplicación web de Sharepoint*
	Nota: Esta configuración en un entorno en producción no es algo trivial, por lo que se deberá realizar un análisis previo de las necesidades y configuraciones establecidas. En muchos entornos será necesario modificar parámetros adicionales de compatibilidad con Internet Explorer o mecanismos de cifrado AES de Kerberos.

ANEXO A.2.3. Asignación de permisos y roles

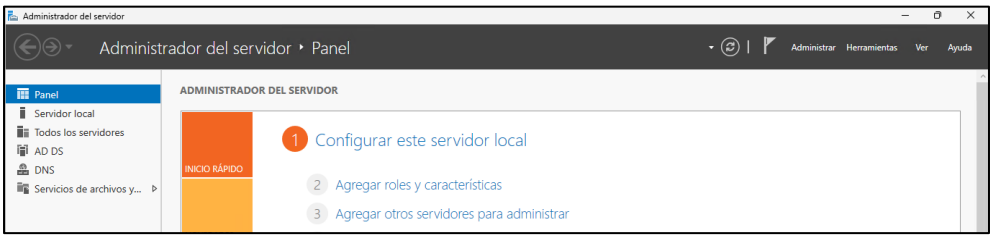
La implementación de Sharepoint Subscription Edition bajo un modelo de control de accesos basado en roles es necesaria para mitigar el riesgo de escalada de privilegios y limitar el área de exposición dentro de una infraestructura. Toda instalación de Sharepoint dispone de un “Administrador Global de la Granja”, punto único de fallo en caso de comprometimiento de la cuenta. Se recomienda segregar las funciones de administración entre dicho usuario y un grupo de administradores del servicio, garantizando de este modo la disponibilidad de gestión y configuración a nivel de sistema. A su vez, cualquier cambio realizado dispondrá de la trazabilidad adecuada, al establecer que los cambios en el esquema de base de datos estén restringidas a un grupo de identidades supervisadas cumpliendo con el principio de menor privilegio.

En la medida que sea posible, se recomienda evitar permisos individuales y la arquitectura de seguridad debe garantizar un aislamiento estricto a nivel de aplicaciones

web mediante la creación de grupos de seguridad granulares para los usuarios finales. Al desvincular los permisos administrativos de los privilegios de acceso a la información final, se evitará el acceso transversal no autorizado entre diferentes unidades de negocio o aplicaciones, lo que prevendrá la fuga de datos accidental al operar en planos de seguridad independientes y aislados.

Nota: Es necesario asegurar que la cuenta de administración e instalación de Sharepoint está configurada siguiendo los mínimos privilegios en Directorio Activo y los servidores SQL. A su vez, la cuenta de servicio de la granja deberá disponer de permisos limitados en los servidores locales o las máquinas que albergan las bases de datos de la infraestructura.

Se realizarán los siguientes pasos para abordar este requerimiento.

Paso	Descripción
1.	En primer lugar, se dará comienzo con la incorporación de un grupo de administradores en la consola de "Administración Central de Sharepoint". Inicie sesión en un controlador de dominio con privilegios de administración.  *Ilustración 129 - Consola de administración del servidor*

2.	Inicie la consola de “Usuarios y equipos de Active Directory”.

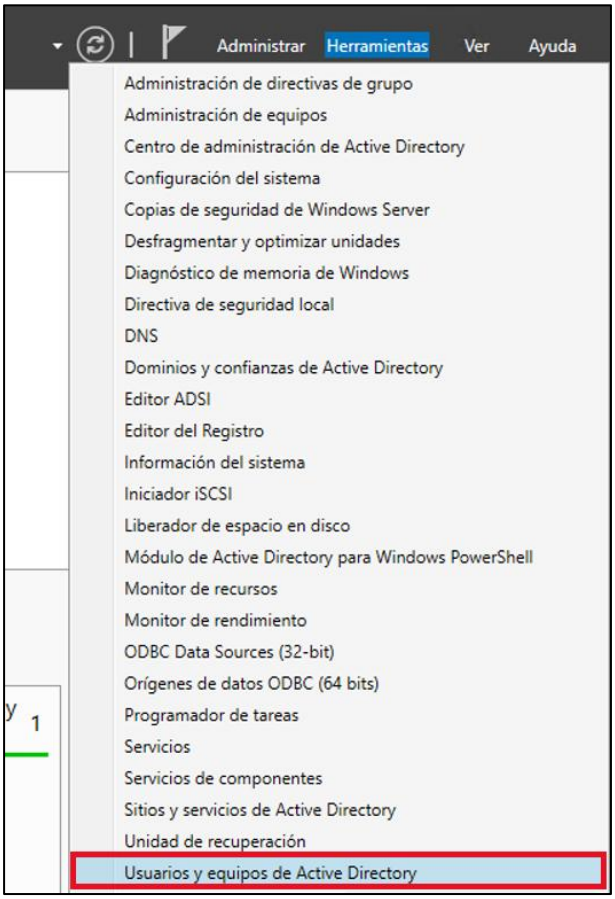


Ilustración 130 - Acceso a la consola de administración de "Usuarios y grupos de directorio activo"

3.	Confirme la existencia de un grupo que contenga los usuarios que administrarán Sharepoint.

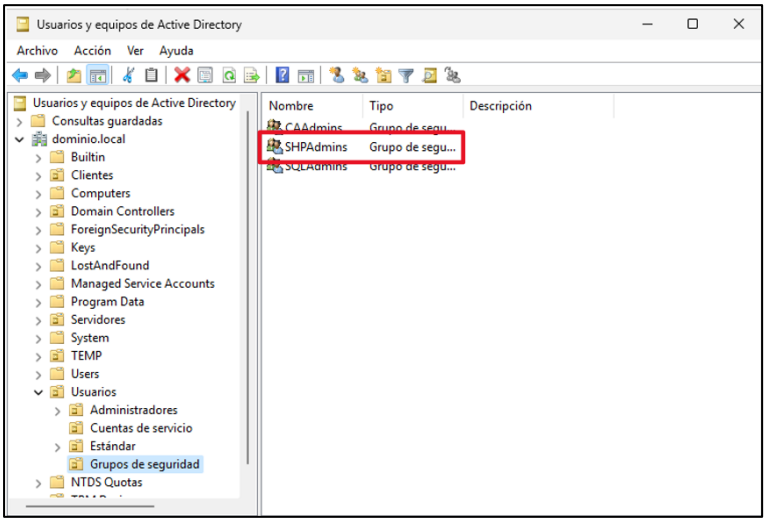
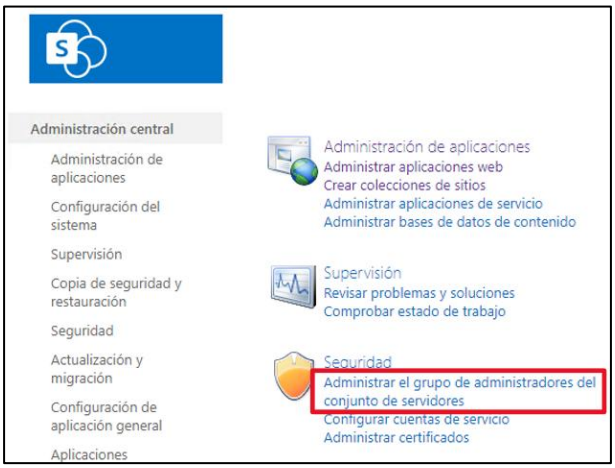
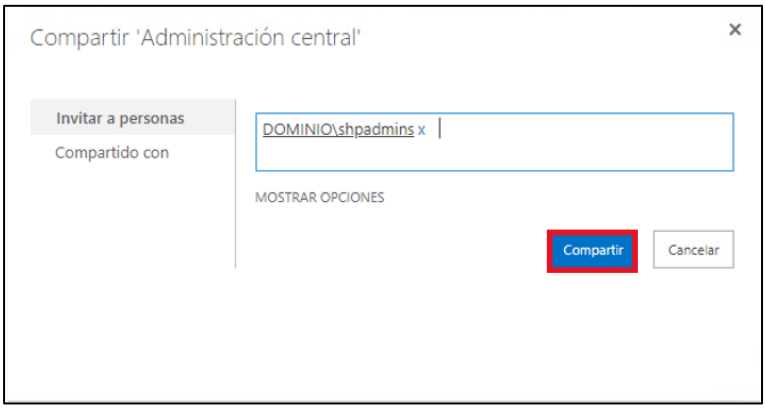
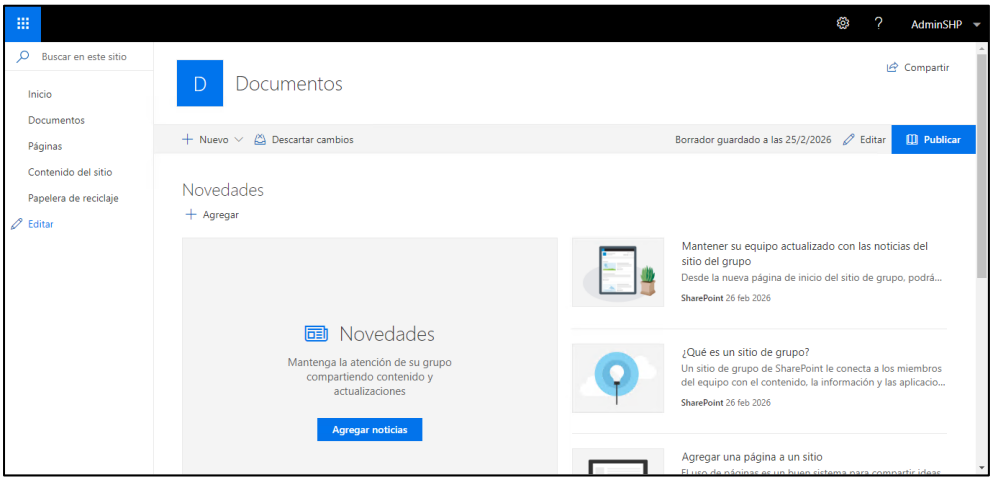
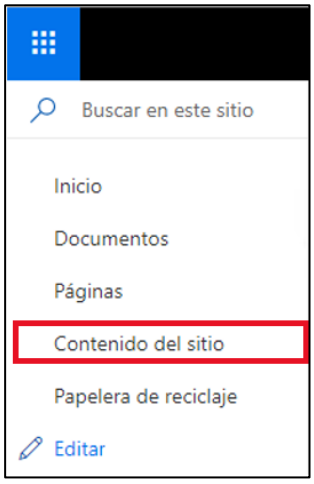


Ilustración 131 - Grupo de seguridad de administración de Sharepoint

	Nota: En este caso, SHPAdmins agrupa las identidades de los usuarios administradores del producto. En caso de no existir, cree un grupo de seguridad para dicho fin.
4.	Cierre la consola de administración en el controlador de dominio y finalice la sesión de Windows.
5.	Inicie sesión en el servidor Sharepoint con un usuario con privilegios de administración o acceda a la consola de "Administración central de Sharepoint" desde un equipo autorizado.  *Ilustración 132 - Consola de Administración central de Sharepoint*
6.	Haga clic en "Administrar el grupo de administradores del conjunto de servidores" en la sección de "Seguridad".  *Ilustración 133 - Acceso a la gestión de administradores de la granja de Sharepoint*
7.	Pulse sobre "Nuevo" para agregar el grupo de administradores a "Farm Administrators".  *Ilustración 134 - Nuevo grupo de administración de la granja*

8.	A continuación, pulse sobre “Agregar usuarios”.  *Ilustración 135 - Agregar grupo de administración*
9.	Introduzca el nombre del grupo de seguridad, y haga clic en “Compartir”.  *Ilustración 136 - Permisos de administración de Sharepoint* **Nota**: Desde este momento, los miembros del grupo de administración de Sharepoint dispondrán de los privilegios necesarios para administrar los servidores de la granja.

10.	Además de administrar los servidores, estos usuarios deberán disponer de permisos de administración de las diferentes colecciones de sitios. No obstante, se puede dar la situación de que los administradores de cada colección difieran de los administradores globales. Para permitir la gestión de los mismos, acceda a cada sitio con un usuario con privilegios de administración.  *Ilustración 137 - Acceso a la colección de sitios*
11.	Haga clic sobre “Contenido del sitio”.  *Ilustración 138 - Contenido del sitio*

12.	A continuación, pulse sobre “Configuración del sitio”.

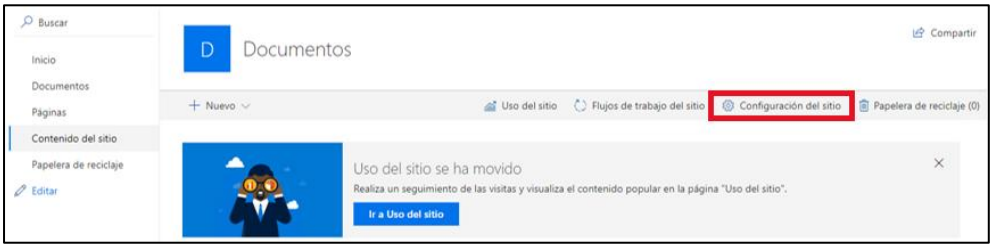


Ilustración 139 - Configuración del sitio

13.	En la sección “Usuarios y permisos”, haga clic en “Administradores de la colección de sitios”.

Ilustración 140 - Administradores de la colección de sitios

14.	Introduzca el grupo deseado, y a continuación, acepte los cambios.

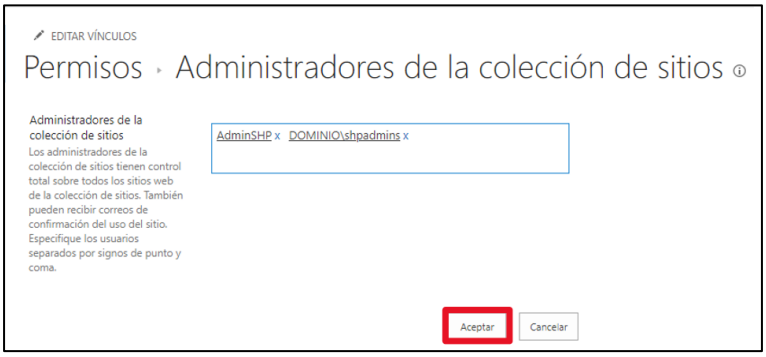


Ilustración 141 - Asignación de administradores de la colección de sitios

15.	A continuación, en la misma sección “Usuarios y permisos”, seleccione “Personas y grupos”.

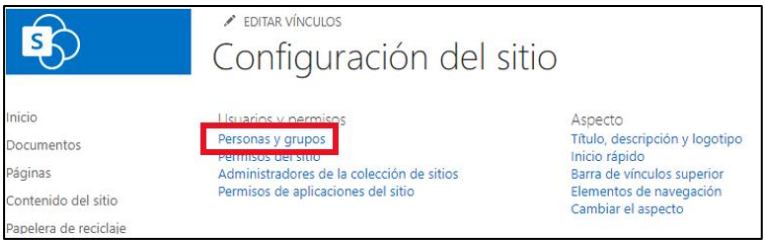


Ilustración 142 - Personas y grupos en Sharepoint

16.	En el panel de la izquierda, pulse sobre “Propietarios documentos”.

Ilustración 143 - Propietarios de documentos

17.	Haga clic en “Nuevo” para agregar el grupo de administración del sitio.

Ilustración 144 - Agregar grupo de administradores

18.	Pulse en “Agregar usuarios”.

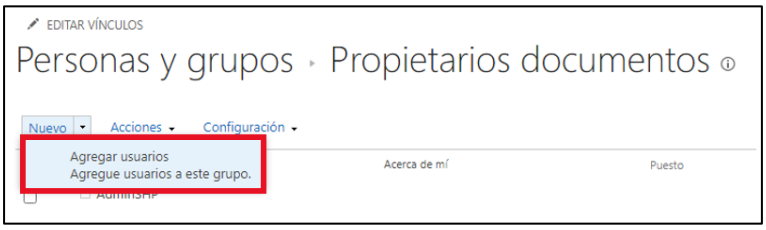


Ilustración 145 - Agregar grupo de administradores

19.	Seleccione el grupo de administración de la colección y pulse en “Compartir”.

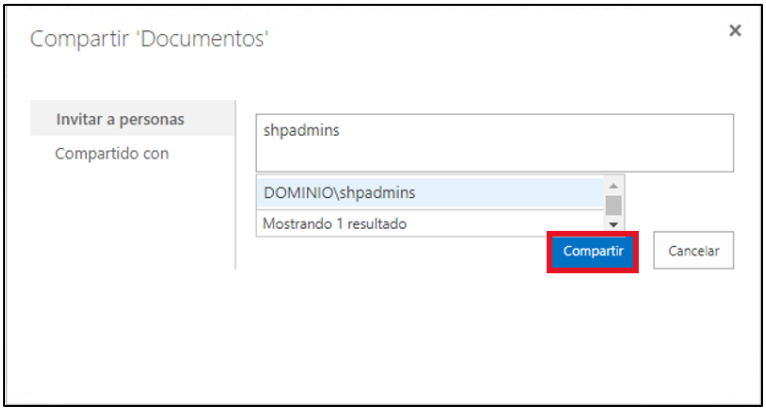
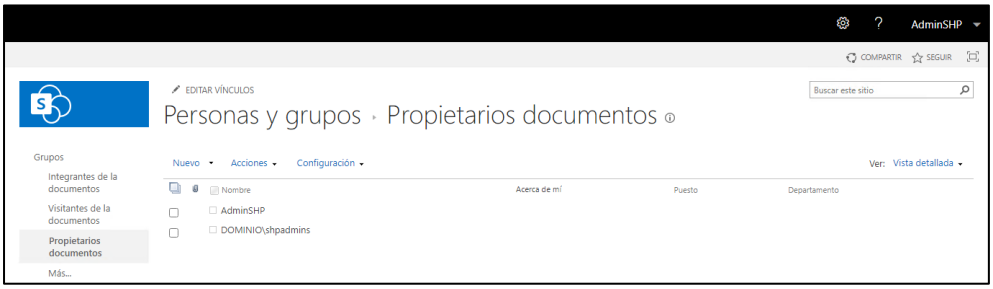
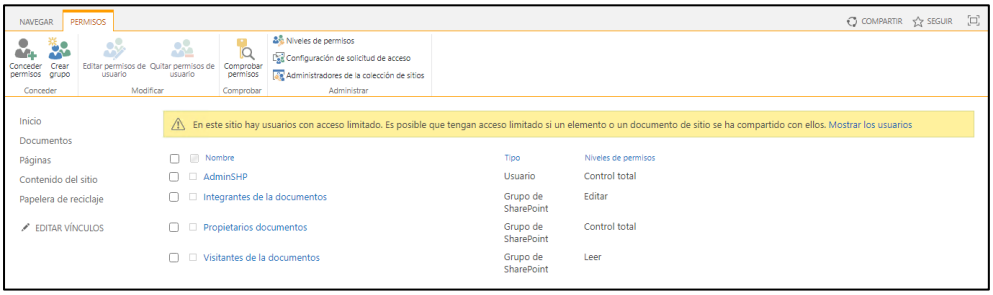


Ilustración 146 - Selección de grupo de administradores

20.	Con esta configuración, los miembros del grupo "SHPAdmins" tendrán privilegios administrativos sobre la colección de sitios, así como la visibilidad de todos los documentos alojados en él.  *Ilustración 147 - Personas y grupos con privilegios de administración en Sharepoint* **Nota**: Como se comenta en líneas anteriores, es una buena práctica que cada colección de sitios disponga de un grupo de administración diferenciado por organizaciones, secciones o departamentos. De este modo, se realizará una separación lógica y se evitará el movimiento transversal entre aplicaciones web de Sharepoint.
21.	Por otro lado, se recomienda la creación de grupos de usuario y proporcionar los permisos de "Visitante" de forma colectiva, y evitar de este modo la herencia no controlada, los accesos no autorizados y mantener una estandarización de accesos bien definida.
22.	Para proporcionar dichos accesos, acceda a "Permisos del sitio".  *Ilustración 148 - Acceso a permisos del sitio*
23.	Haga clic sobre el grupo deseado, facilitando así la edición o únicamente el consumo de la información con permisos de solo lectura.  *Ilustración 149 - Selección de "Visitantes de los documentos"*

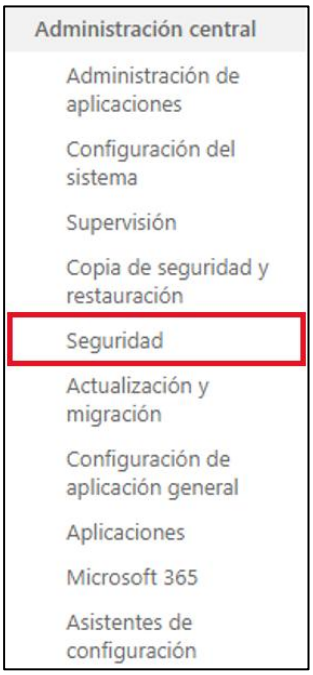
24.	Agregue el grupo pulsando sobre el botón “Nuevo” y siguiendo los pasos anteriores.

Ilustración 150 - Compartir el sitio al grupo de visitantes

Ilustración 151 - Compartir el sitio al grupo de visitantes

ANEXO A.2.4. Seguridad de elementos Web

El objetivo de la siguiente configuración es reducir la superficie de exposición sobre el servicio y bloquear la ejecución de elementos web no autorizados. Esta directiva implementa un control de seguridad a nivel de granja que restringe la ejecución de elementos web exclusivamente a componentes desplegados por el administrador del sistema, forzando a Sharepoint a utilizar únicamente los recursos almacenados en el repositorio local de la infraestructura. Se deshabilita la resolución de dependencias externas hacia la galería en línea de Microsoft, garantizando la operación bajo un modelo de aislamiento de red.

Paso	Descripción
1.	Para realizar la configuración descrita, acceda a la consola de "Administración central de Sharepoint" con un usuario con privilegios administrativos.  *Ilustración 152 - Consola de Administración central de Sharepoint*
2.	Haga clic en "Seguridad", localizado en el menú de administración central.  *Ilustración 153 - Acceso a las configuraciones de seguridad*

3.	En la sección “Seguridad general”, seleccione “Administrar la seguridad de elementos web”.  *Ilustración 154 - Administrar la seguridad de elementos web*
4.	En el menú desplegable de Aplicación web, seleccione la aplicación donde desea establecer la configuración.  *Ilustración 155 - Seleccionar la aplicación web* **Nota**: Tenga en cuenta que en entornos productivos podría impactar en la funcionalidad existente. Si las aplicaciones utilizan elementos web dependientes de esta galería en línea, dejarán de funcionar inmediatamente.

5.	Seleccione “Impedir que los usuarios tengan acceso a la Galería en línea de elementos web y ayudar a mejorar la seguridad y el rendimiento”. A continuación, pulse en “Aceptar”

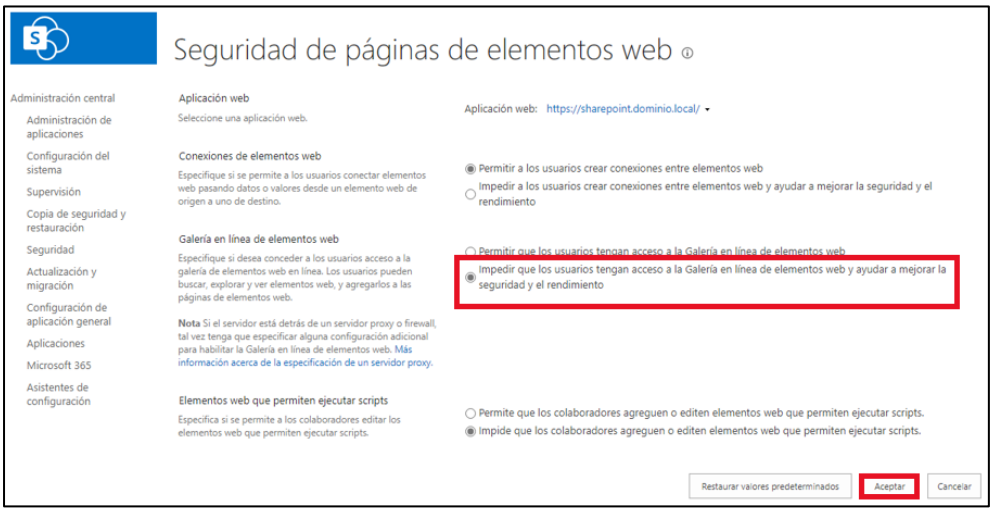
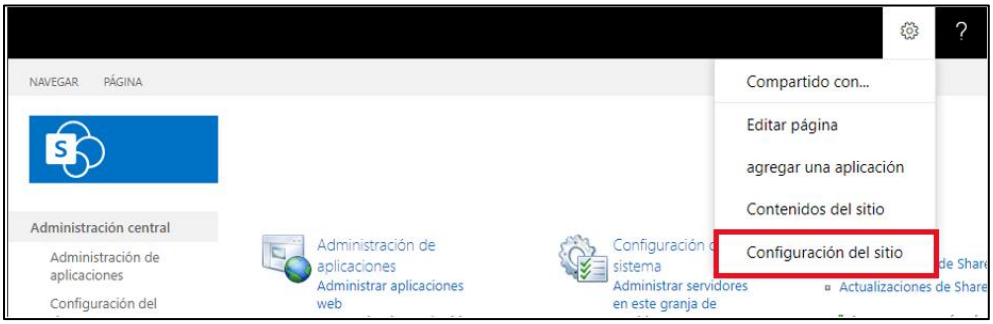


Ilustración 156 - Impedir el acceso a elementos web

ANEXO A.2.5. Configuración de auditoría

Se garantizará al menos un periodo de retención mínima de 90 días para los registros de auditoría de Sharepoint, asegurando la trazabilidad necesaria para la reconstrucción de eventos y el cumplimiento de los estándares de seguridad institucional. La existencia de un historial de logs permitirá la identificación de investigación de posibles incidentes.

Paso	Descripción
1.	Para habilitar la auditoría, acceda a la consola de “Administración central de Sharepoint” con un usuario con privilegios de administrador.  *Ilustración 157 - Consola de Administración central de Sharepoint*
2.	Haga clic en el engranaje de herramientas y posteriormente, en “Configuración del sitio”.  *Ilustración 158 - Acceso a configuración del sitio*

3.	En la sección de “Administración de la colección de sitios”, seleccione “Configuración de auditoría de la colección de sitios”.

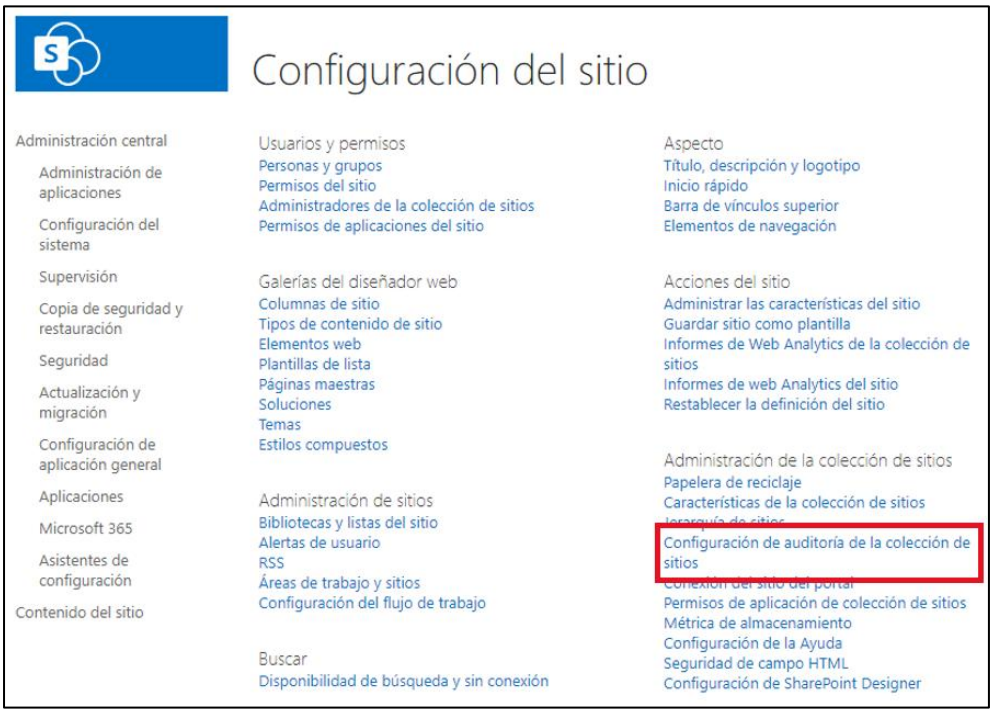


Ilustración 159 - Configuración de auditoría

4.	Defina los eventos que deben ser auditados según los requisitos de su organización. A continuación, pulse en “Aceptar”.

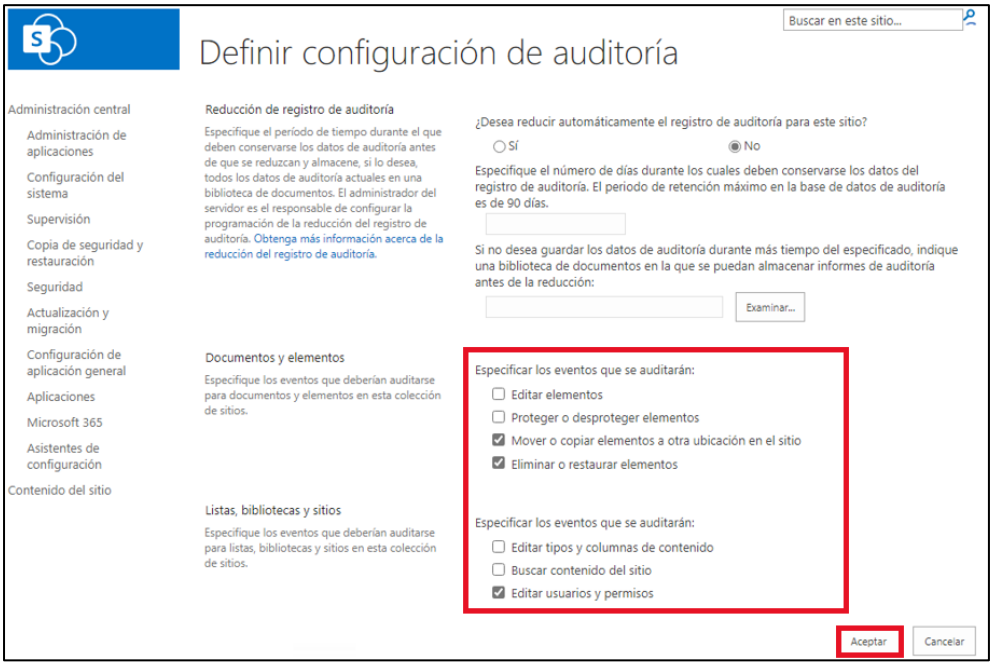


Ilustración 160 - Definir la configuración de auditoría

ANEXO A.2.6. Antivirus en Sharepoint

Como parte de los protocolos de configuración de seguridad de los sistemas, se establece como requisito obligatorio la configuración de medidas anti ransomware de Sharepoint. La ejecución de escaneo de documentos previene la difusión de software malintencionado. Esta implementación es necesaria para validar la seguridad de los elementos integrados por los usuarios, permitiendo el aislamiento preventivo de elementos maliciosos y reduciendo la superficie de exposición ante incidentes de ransomware.

Para habilitar el componente de antivirus de Sharepoint, se seguirán los siguientes pasos.

Paso	Descripción
1.	Acceda a la consola de “Administración central de Sharepoint” con un usuario con privilegios de administrador.  *Ilustración 161 - Consola de Administración central de Sharepoint*

2.	Haga clic en la sección “Seguridad”.

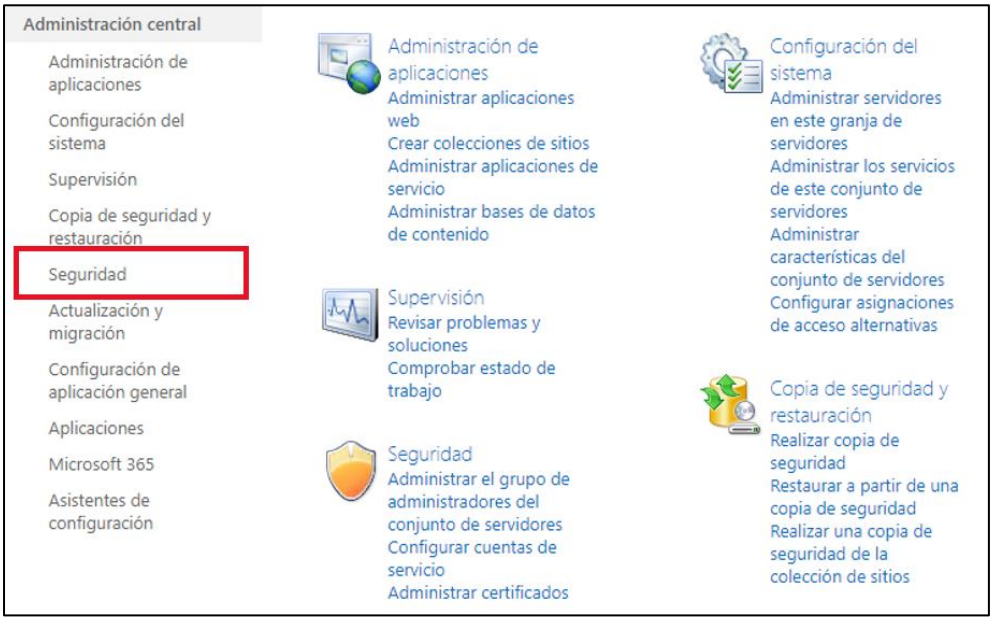


Ilustración 162 - Acceso a la sección de Seguridad

3.	Seleccione “Administrar la configuración del antivirus” en “Seguridad general”.

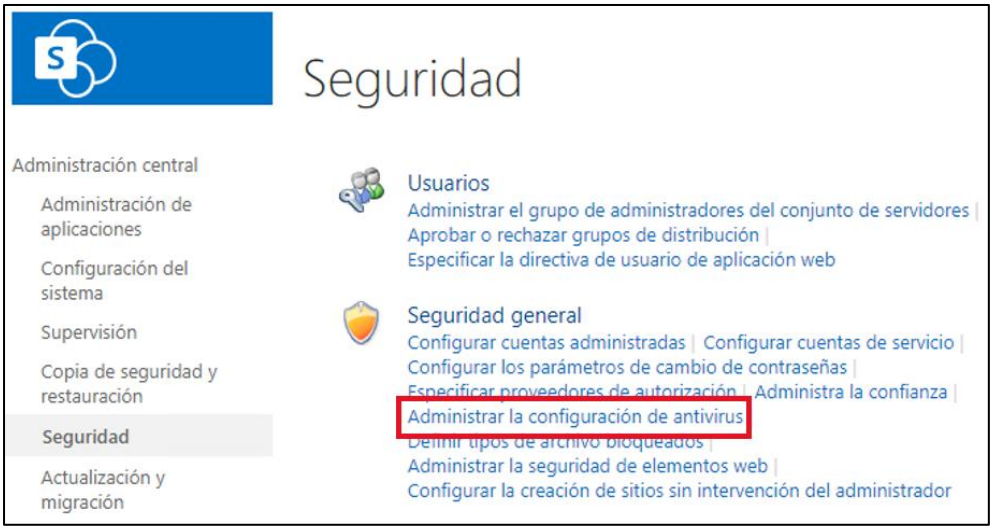


Ilustración 163 - Configuración del antivirus de Sharepoint

4.	Marque las opciones “Examinar documentos al cargarlos”, “Examinar documentos al descargarlos” e “Intentar limpiar los documentos infectados”. Dejando desactivado el campo “Permitir a los usuarios descargar documentos infectados”. Para finalizar, pulse “Aceptar”.

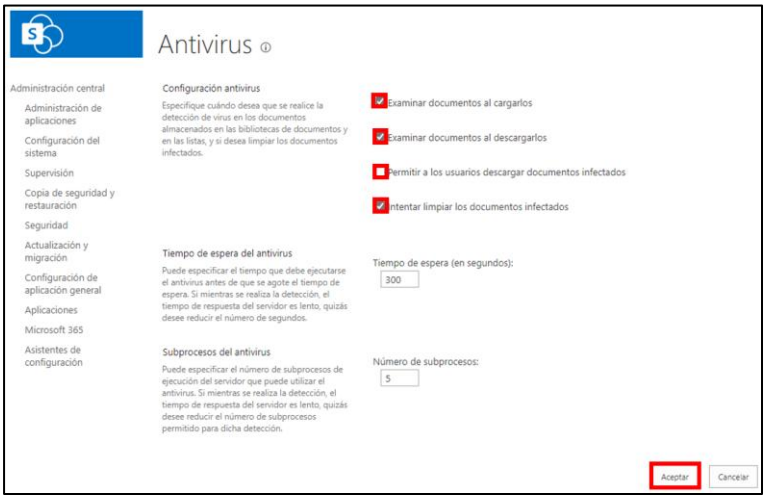


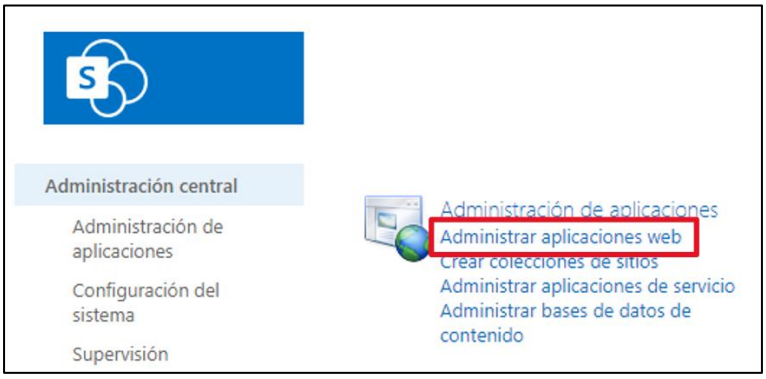
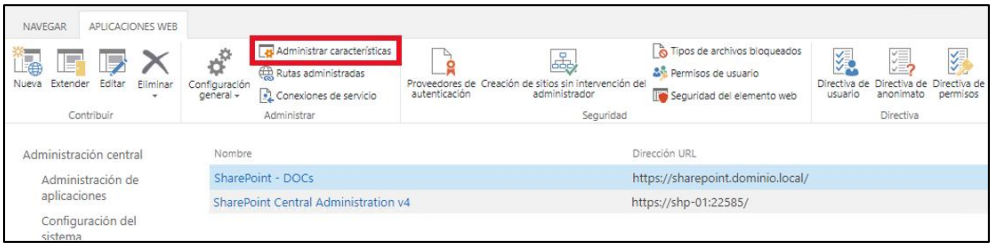
Ilustración 164 - Configuración de antivirus en Sharepoint

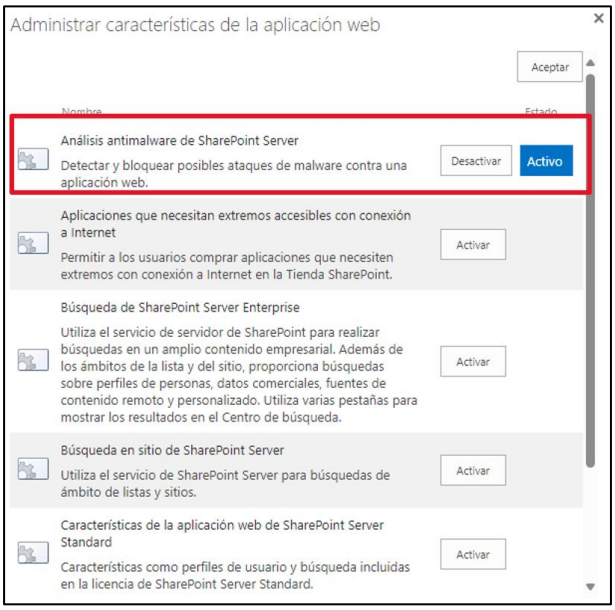
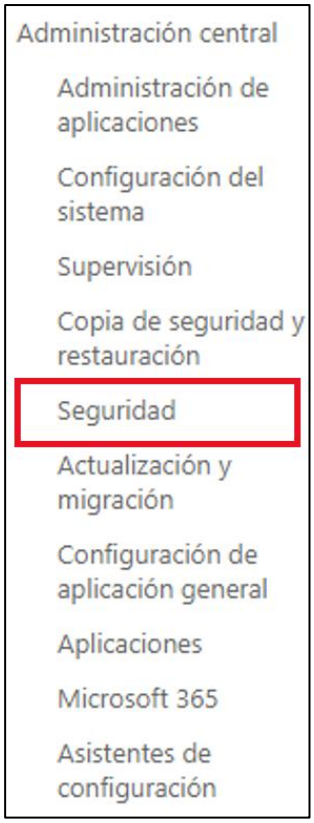
ANEXO A.2.7. Análisis AMSI en Sharepoint

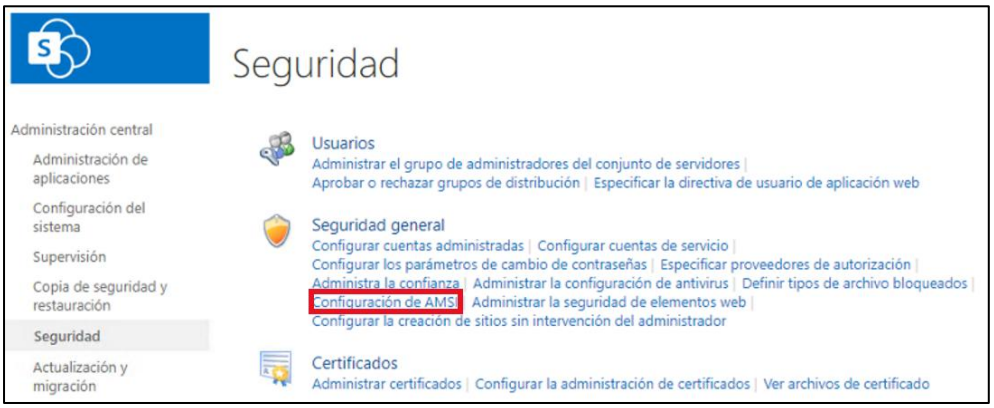
De manera complementaria al “Anexo A.2.6. Antivirus en Sharepoint” anterior, se ha introducido una nueva “Interfaz de examen antimalware (AMSI)” en versiones modernas de Sharepoint Subscription Edition. A causa de la modernización de la situación actual de la ciberseguridad, los ataques complejos a gran escala están en aumento. AMSI es un estándar versátil que permite a las aplicaciones y servicios integrarse con cualquier producto antimalware compatible con AMSI presente en los equipos.

La integración entre un antivirus compatible con AMSI y Sharepoint permitirá el análisis en tiempo real de las peticiones HTTP y HTTPS, impidiendo que el servidor de la infraestructura procese solicitudes peligrosas.

Nota: Para habilitar AMSI, se deberá disponer al menos de la versión Sharepoint Subscription Edition 22H2 o posterior.

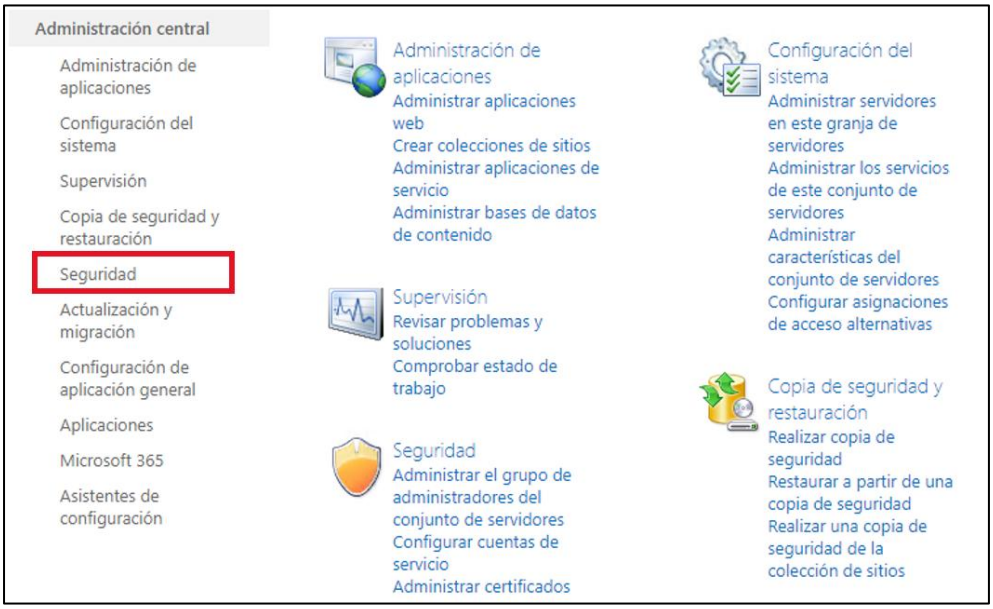
Paso	Descripción
1.	Acceda a la consola de “Administración central de Sharepoint” con un usuario con privilegios de administrador.  *Ilustración 165 - Consola de Administración central de Sharepoint*
2.	Acceda a “Administrar aplicaciones web” en la sección de administración de aplicaciones.  *Ilustración 166 - Administrar aplicaciones web*
3.	Seleccione la aplicación web donde desee habilitar AMSI y, a continuación, pulse en “Administrar características”.  *Ilustración 167 - Administración de características*

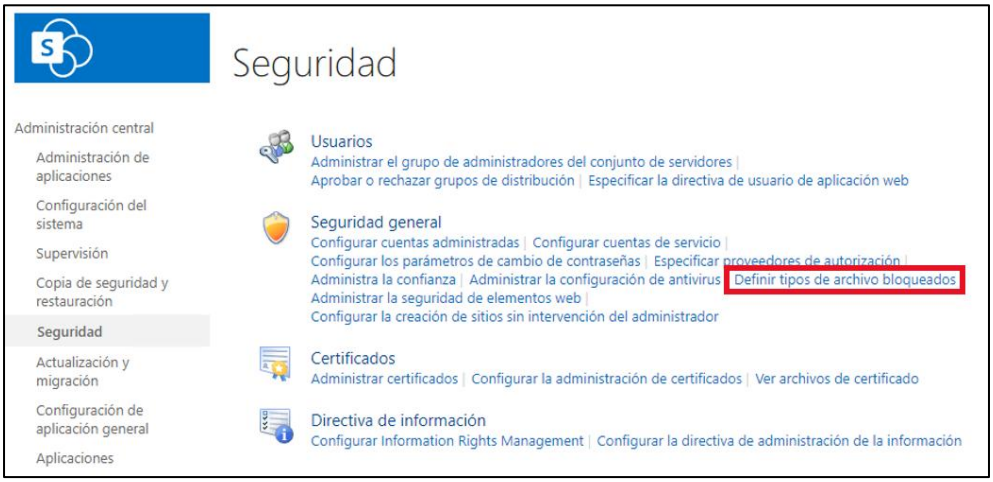
4.	Confirme que el "Análisis antimalware de Sharepoint Server" se encuentra "Activo".  *Ilustración 168 - Análisis antimalware de Sharepoint*
5.	A continuación, acceda a "Seguridad" en el menú de administración central.  *Ilustración 169 - Acceso al menú de seguridad de Sharepoint*

6.	Pulse sobre la característica de “Configuración de AMSI”.  *Ilustración 170 - Configuración AMSI*
7.	Confirme que la característica de detección se encuentra habilitada.  *Ilustración 171 - Confirmación de configuración AMSI* **Nota**: Si no se encuentra habilitada, marque dicha opción y a continuación, pulse en “Aceptar”.

ANEXO A.2.8. Filtrado de tipos de archivo

Con el fin de evitar la descarga de archivos con extensiones que puedan ser fuente de infecciones o contener software malicioso, se establecerá el bloqueo de extensiones. Se trata de filtrar archivos peligrosos o vectores de ataque que permitan la ejecución de código arbitrario o escalación de privilegios, como por ejemplo binarios autoejecutables, scripts o contenedores de metadatos.

Paso	Descripción
1.	Para establecer el filtro de archivos, acceda a la consola de "Administración central de Sharepoint" con un usuario con privilegios de administrador.  *Ilustración 172 - Consola de Administración central de Sharepoint*
2.	Haga clic en la sección "Seguridad".  *Ilustración 173 - Acceso a la sección Seguridad*

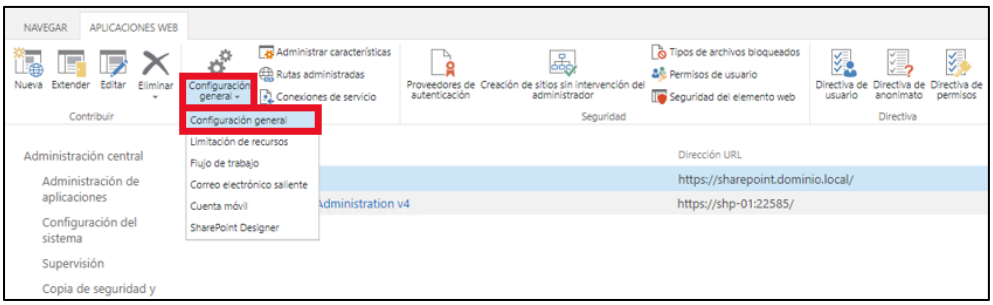
3.	Pulse en “Definir tipos de archivo bloqueados”.  *Ilustración 174 - Definir tipos de archivo bloqueados*
4.	Introduzca las extensiones de archivo que desee bloquear en líneas diferentes. A continuación, pulse en “Aceptar”.  *Ilustración 175 - Tipos de archivo bloqueados*

ANEXO A.2.9. Tiempo de inactividad de la sesión

Cada vez que se inicia una sesión de usuario de SharePoint, se genera un identificador de sesión único y otra información de la sesión. Esta información puede ser utilizada por un usuario malintencionado para secuestrar la sesión. Al finalizar las sesiones y alcanzar el límite de tiempo de inactividad, se invalida la información subyacente de la sesión. Por lo tanto, se elimina la posibilidad de secuestro de la sesión.

Un bloqueo de sesión por tiempo de espera es una acción temporal que se toma cuando un usuario deja de trabajar, pero no cierra la sesión debido a la naturaleza temporal de la ausencia. A nivel de sistema operativo se suelen tomar medidas para

iniciar el bloqueo de sesión, pero Sharepoint también es capaz de realizarlo a nivel de aplicación. Es posible definir el bloqueo tras el periodo de inactividad antes de un bloqueo de sesión de sistema.

Paso	Descripción
1.	Para establecer el filtro de archivos, acceda a la consola de "Administración central de Sharepoint" con un usuario con privilegios de administrador y en la sección de "Administración de aplicaciones", pulse sobre "Administrar aplicaciones web".  *Ilustración 176 - Consola de Administración central de Sharepoint*
2.	Seleccione la aplicación donde se establecerá el bloqueo de inactividad y pulse en "Configuración general". A continuación, pulse en "Configuración general".  *Ilustración 177 - Configuración general de la aplicación web*

3.	Diríjase a la sección de “Validación de seguridad de página web” y establezca el tiempo de expiración de validación.

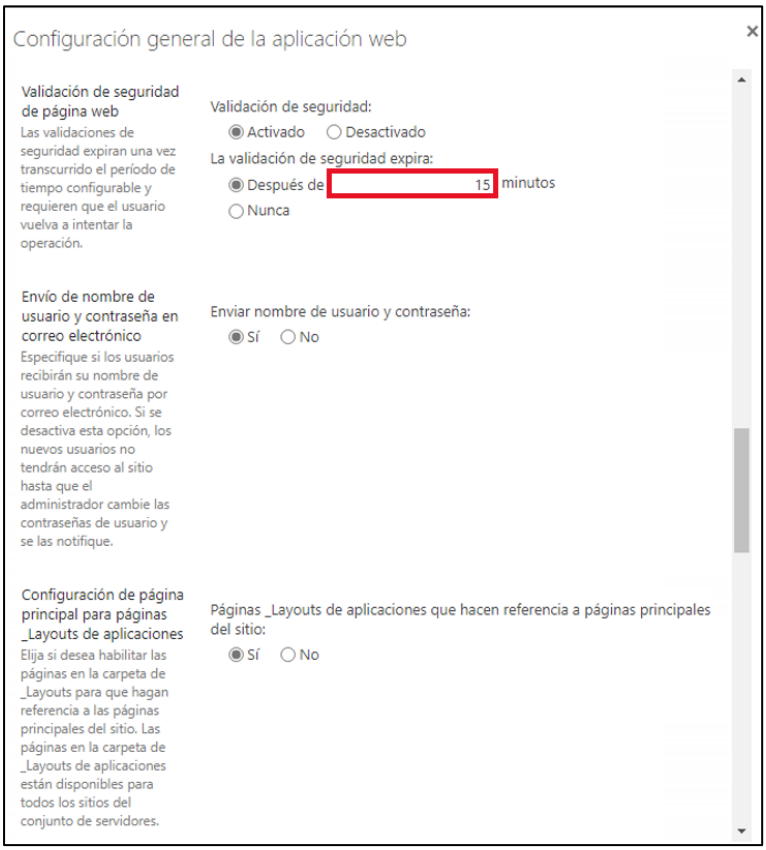


Ilustración 178 - Validación de seguridad de página web

4.	A continuación, desplácese al final de la ventana de configuración y pulse en “Aceptar”.

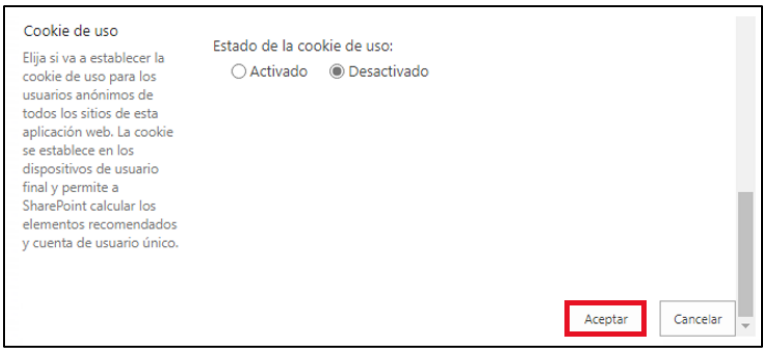
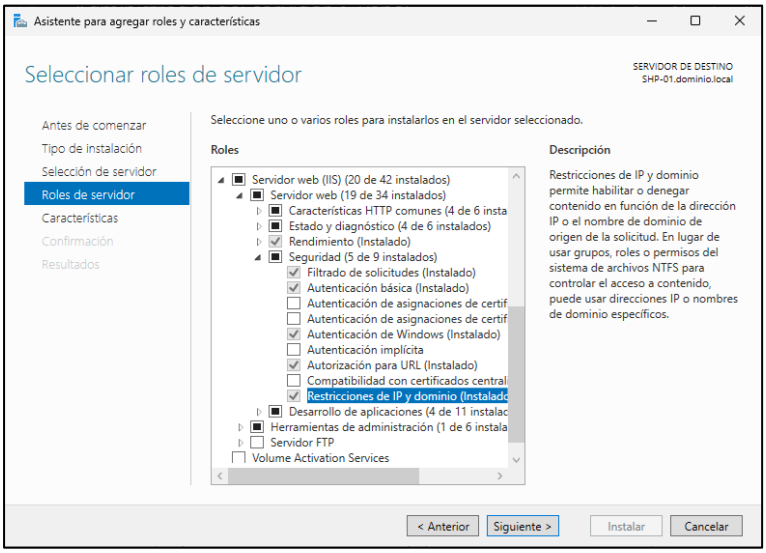


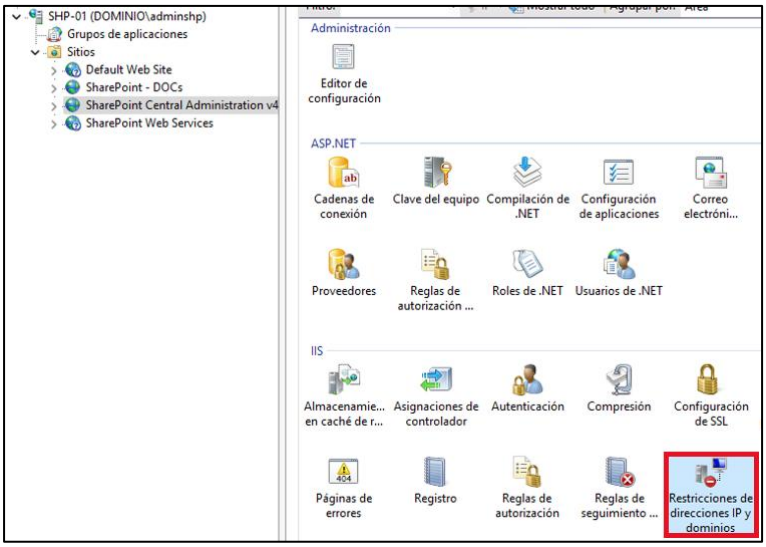
Ilustración 179 - Aceptar la configuración establecida

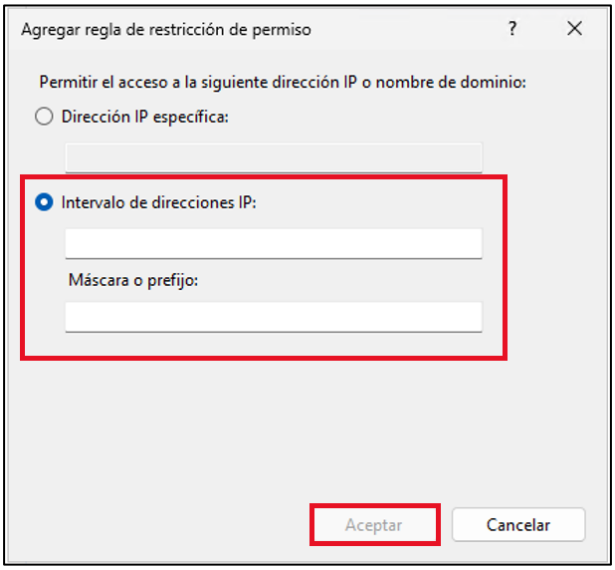
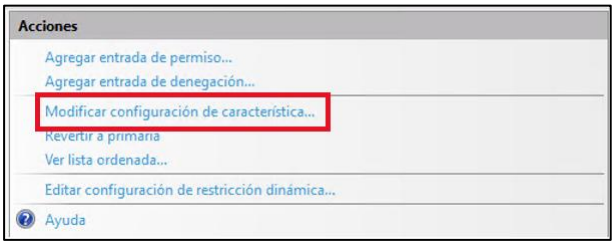
ANEXO A.2.10. Restricciones de acceso

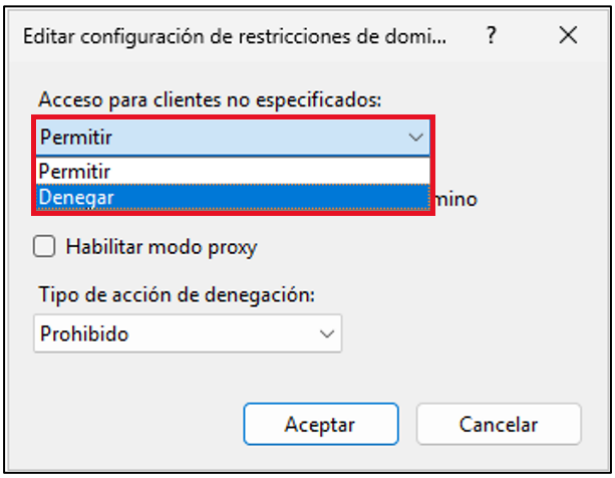
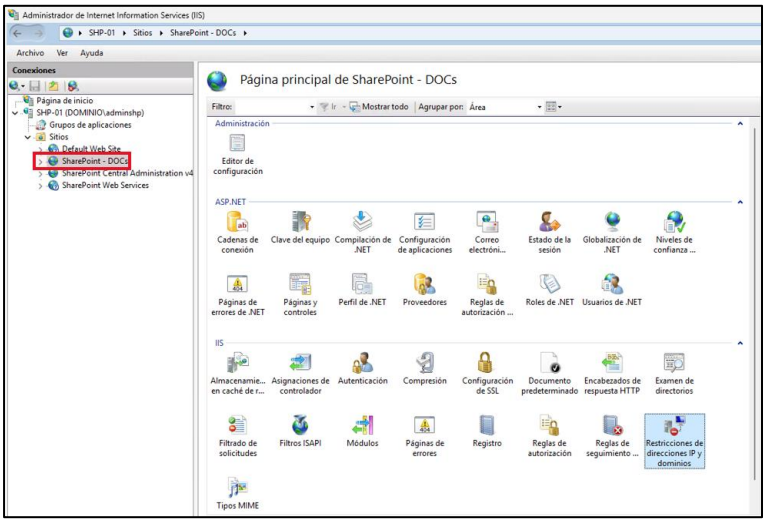
La utilización de "Internet Information Services (IIS)" como motor web para Sharepoint y la aplicación de medidas de seguridad sobre la característica con la guía CCN-STIC-574A25, ofrece la posibilidad de aplicar el mínimo privilegio a nivel de red implementando restricciones de acceso basadas en IP y nombres de dominio. Es altamente recomendable la segregación del tráfico hacia la consola de Administración central de Sharepoint y las distintas aplicaciones web existentes. Esta configuración establecerá una capa de defensa perimetral a nivel de red que reducirá el área de exposición, evitando que los puntos de acceso críticos no queden expuestos a redes no autorizadas o segmentos de red de usuarios o propósito general.

Estas restricciones actuarán como filtro previo con el objetivo de evitar el establecimiento de conexiones no legítimas o ataques de denegación de servicio (DoS).

Paso	Descripción
1.	Acceda al servidor en el que se encuentra instalado el producto Sharepoint Subscription Edition con privilegios de administración.
2.	Confirme que el servidor IIS ha sido bastionado con la guía "CCN-STIC-574A25 Aplicación de seguridad Microsoft Internet Information Services (IIS) 10", o al menos, la característica "Restricciones de IP y dominio" se encuentra instalada.  *Ilustración 180 - Restricciones de IP y dominio*

3.	Inicie el “Administrador de Internet Information Services (IIS)”.  *Ilustración 181 - Consola de Administración de IIS*
4.	Seleccione “SharePoint Central Administration v4” y haga doble clic en “Restricciones de direcciones IP y dominios”.  *Ilustración 182 - Acceso a "Restricciones de direcciones IP y dominios"*
5.	En el menú de Acciones situado en la parte derecha, haga clic sobre "Agregar entrada de permiso…" o "Agregar entrada de denegación…", según la política que se haya definido. En este caso, se seleccionará la primera de ellas, para indicar la red de administración del sistema y que, por lo tanto, podrá acceder a la consola de gestión de Sharepoint.  *Ilustración 183 - Agregar entrada de permiso de acceso*

6.	A continuación, se introducirá la dirección IP específica o el segmento red de administración desde donde se accederá a la consola de Administración Central de Sharepoint. Para guardar el cambio, pulse en “Aceptar”.  *Ilustración 184 - Establecer intervalo de direcciones IP* **Nota**: En entornos seguros, se recomienda la creación de redes de administración de la infraestructura, así como redes de administración del entorno, que permitirán el acceso a los servicios y productos.
7.	Tras establecer los permisos de acceso a la red deseada, hacer clic en “Modificar configuración de característica” en el menú de “Acciones”.  *Ilustración 185 - Modificar la configuración de la característica*

8.	En el desplegable “Acceso para clientes no especificados”, seleccione la opción “Denegar”, y posteriormente, “Aceptar”.  *Ilustración 186 - Configuración de la característica*
9.	Esta configuración permitirá únicamente el acceso a la consola de administración de Sharepoint desde la red especificada, bloqueando la exposición del frontal a redes no definidas en la entrada de permiso.
10.	De igual modo, esta configuración se deberá realizar en las diferentes aplicaciones web existentes en Sharepoint. Así, se limitará el acceso a los contenidos de las colecciones de sitio exclusivamente desde redes con origen conocido.  *Ilustración 187 - Modificación de aplicaciones web* **Nota**: Esta configuración deberá ser controlada para evitar impactar en los accesos a la documentación o administración del sistema. Si no conoce la red o subred donde se alojan los equipos, consulte con su administrador de redes. Es posible agregar tantas reglas como redes configuradas en su entorno.

ANEXO A.2.11. Prevención de ejecución de código

Sharepoint dispone de medidas de seguridad diseñadas para proteger a los usuarios de contenido malicioso que podría ejecutarse directamente desde el navegador. Una de ellas es el establecimiento del modo "Estricto" en la configuración de manejo de archivos del explorador. De manera predeterminada, Sharepoint configura el modo "Estricto" en todas sus aplicaciones web.

La herramienta agrega encabezados con el objetivo de forzar la descarga de ciertos tipos de archivo. De este modo denegará que el navegador los abra automáticamente evitando ataques de Cross-Site Scripting y la ejecución instantánea de contenido susceptible de ser malicioso como Java, JavaScript o ActiveX.

Paso	Descripción
1.	Para confirmar que el manejo de archivos del explorador no ha sido modificado, y está establecido en modo "Estricto", acceda a la consola de "Administración central de Sharepoint" con un usuario con privilegios de administración.  *Ilustración 188 - Consola de Administración central de Sharepoint*

2.	Acceda a “Administrar aplicaciones web” en la sección de “Administración de aplicaciones”.

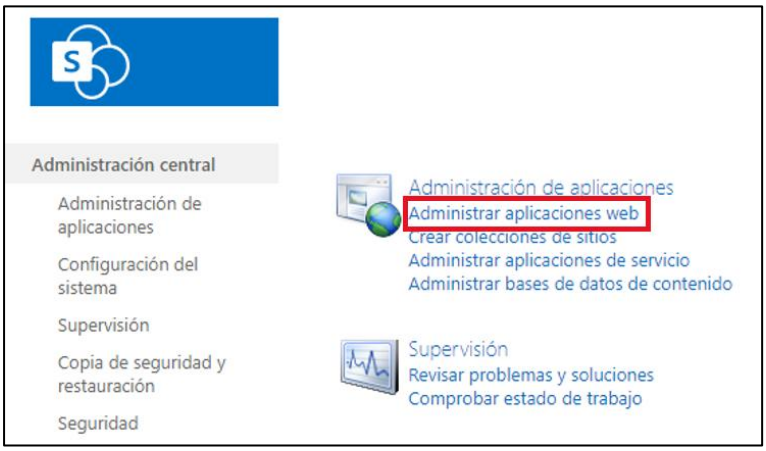


Ilustración 189 - Acceso a la administración de aplicaciones web

3.	Seleccione la aplicación web donde se realizará la comprobación, y a continuación, pulse en “Configuración general” como muestra la siguiente imagen.

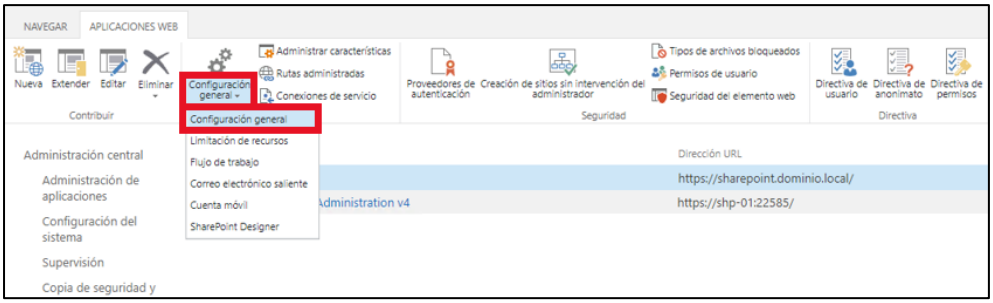
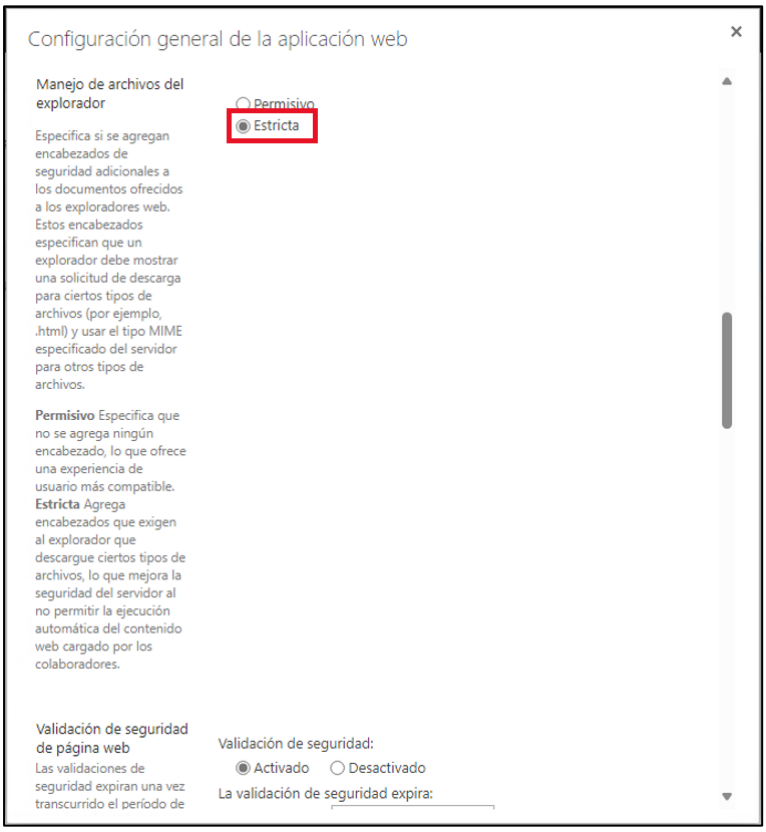
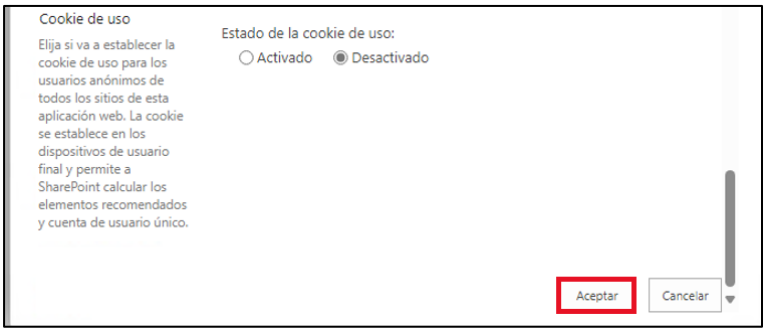


Ilustración 190 - Acceso a Configuración general

4.	Desplácese hasta la sección de “Manejo de archivos del explorador” y confirme que el modo “Estricto” se encuentra habilitado.  *Ilustración 191 – Manejo de archivos del explorador* **Nota**: Si no se encuentra habilitado, marque el selector de “Estricta”.
5.	A continuación, en la parte inferior del menú, pulse en “Aceptar”.  *Ilustración 192 – Aceptar cambios en la configuración*

PUBLICACIONES DE DEFENSA

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