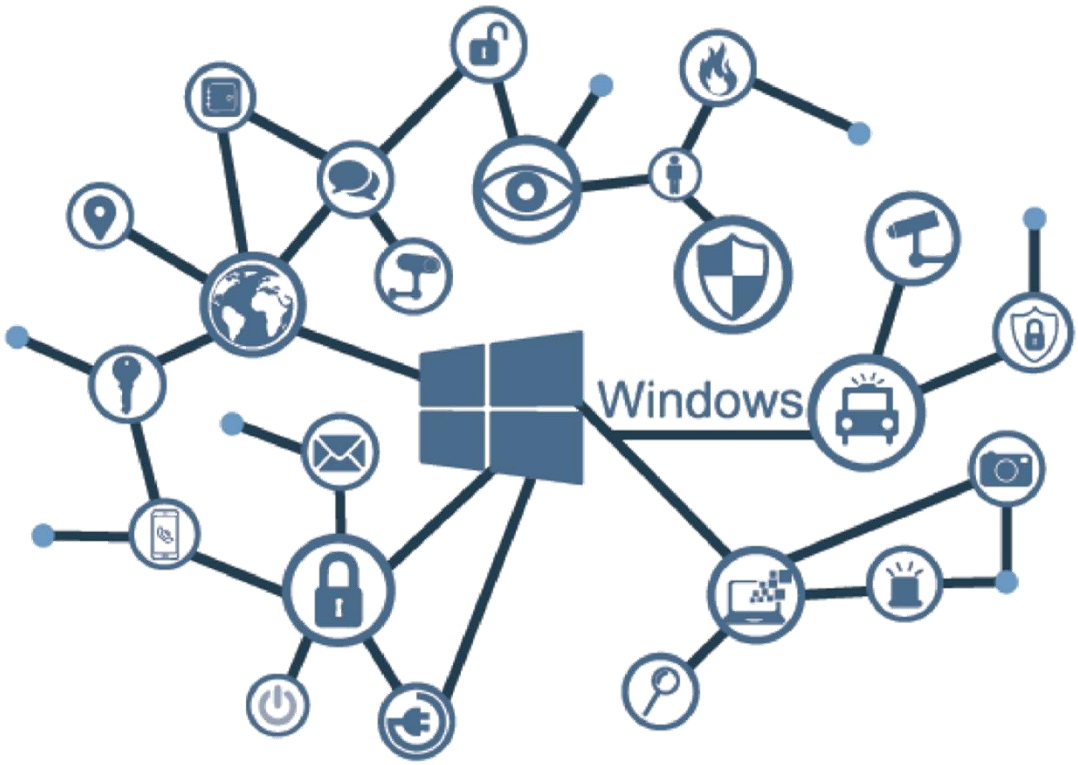
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 574A25

APLICACIÓN DE SEGURIDAD SOBRE MICROSOFT INTERNET INFORMATION SERVICES



ENERO 2026

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

Firmado digitalmente por CCN
Nombre de reconocimiento (DN): c=ES, l=MADRID, o=CCN, ou=SELLO ELECTRONICO, 2.5.4.97=VATES-S2800155J, serialNumber=S2800155J, cn=CCN
Fecha: 2026.09.09 13:23:00 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO 083-26-270-X (edición en línea)

Fecha de Edición: enero de 2026

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

INDICE

1. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el **Centro Criptológico Nacional (en adelante, CCN)** para entornos basados en los productos y sistemas operativos de Microsoft (CCN-STIC-500), siendo de aplicación para la administración pública en el cumplimiento del **Esquema Nacional de Seguridad** (en adelante, ENS) y, de igual modo, de obligado cumplimiento para los sistemas que manejen **Información Clasificada** de ámbito NACIONAL tal y como se expone en el "Artículo 2" del propio ENS. Esto último sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa de aplicación. De igual modo se aplica a los sistemas de información de las entidades del sector privado cuando, según el ENS, "de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público".

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

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

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

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

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

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

2. OBJETO

El propósito de esta guía de seguridad es proporcionar los elementos y directrices para aplicar y garantizar la seguridad en equipos que implementen el aplicativo **Microsoft Internet Information Services 10** (10.0), instalado en un servidor miembro Windows Server 2025 perteneciente a un dominio Windows Server de Directorio Activo.

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

La definición de las medidas de seguridad asociadas a la presente guía se basan, principalmente, en las disposiciones establecidas por el CCN en la Instrucción Técnica de Seguridad de las TIC (CCN-STIC-301) y otras normativas nacionales de aplicación.

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, la probabilidad de materialización de la amenaza y la superficie de exposición del sistema.
- Será adaptable en la aplicación de medidas, evitando una aplicación monolítica y estanca utilizando la Declaración de Aplicabilidad Técnica o Perfil de Cumplimiento Técnico Específico (en adelante, PCTE) como elemento fundamental sobre el que vertebrar la seguridad. Se tomará de igual modo en cuenta el Perfil de Cumplimiento Específico (en adelante, PCE) aplicable al conjunto del organismo y sus sistemas de información.
- El PCTE y las medidas establecidas por medio del presente documento cumplen los requisitos técnicos para que los sistemas TIC se adapten a cualquier CLASIFICACIÓN DE LA INFORMACIÓN tomando en consideración la categorización de los sistemas definida en el ENS.
- Las guías se revisarán y se actualizarán según las nuevas amenazas, avances tecnológicos y estado de arte tecnológico en ciberseguridad, así como nuevas configuraciones de seguridad proporcionadas por los productos.

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

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

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

3. ALCANCE

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

El escenario en el cual está basada la guía CCN-STIC-574A25 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) Un controlador de dominio basado en Windows Server 2025.

e) Dos servidores miembros del dominio 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 Internet Information Services. Completa descripción de los mecanismos de seguridad, autenticación y autorización utilizados en Microsoft IIS 10.

d) Guía paso a paso. Permite implementar y establecer las configuraciones de seguridad necesarias en una arquitectura de un servidor con Microsoft Internet Information Services

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.

- **Configuración de seguridad sobre AD DS:** Las configuraciones de seguridad del servicio y de los componentes necesarios del sistema se modifican por medio de objetos de política de grupo (GPO). Dicha configuración está desarrollada en el anexo *ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE INTERNET INFORMATION SERVICES 10 SOBRE WINDOWS SERVER 2025.*
- **Configuraciones adicionales de seguridad:** Las configuraciones adicionales de seguridad hacen referencia a algunos ajustes que no se pueden realizar mediante aplicación de objetos de política de grupo. Dicha configuración está desarrollada en el anexo *ANEXO A.2. CONFIGURACIONES ADICIONALES DE SEGURIDAD.*

4.1. REQUISITOS PREVIOS PARA INTERNET INFORMATION SERVICES

Antes de aplicar las medidas descritas en esta guía, es necesario que el servidor disponga de un sistema operativo compatible. Internet Information Services (IIS) 10 se encuentra integrado como rol nativo en Windows Server 2025, en las ediciones que permiten la instalación de roles y características de servidor. El sistema debe estar correctamente instalado y actualizado, con una configuración básica funcional que incluya los siguientes elementos:

- Nombre de equipo.
- Resolución DNS.
- Sincronización horaria.
- Conectividad de red.

Asimismo, el servidor debe contar con recursos hardware suficientes para soportar el servicio web y las aplicaciones que se vayan a alojar, así como con la configuración de red y seguridad necesaria. Esto incluye la disponibilidad de los puertos requeridos (habitualmente HTTP y HTTPS), las correspondientes reglas de cortafuegos y, en caso de utilizar comunicaciones cifradas, la disponibilidad de certificados digitales válidos o acceso a la infraestructura de certificación.

5. PERFILADO DE CUMPLIMIENTO TÉCNICO

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

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

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

a) ENS.

b) Difusión Limitada.

c) Información Clasificada.

Con el objetivo de facilitar la implementación de la configuración de seguridad definida bajo el presente documento, en la próxima 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	✗	✗	✓

En los apartados siguientes se desarrollarán los controles específicos aplicables a Microsoft Internet Information Services, 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 Internet Information Services, 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 INTERNET INFORMATION SERVICES

El presente anexo detalla el procedimiento técnico para la configuración de las medidas de seguridad exigidas en entornos de producción basados en Microsoft Windows Server 2025 con Internet Information Services (IIS).

Este despliegue tiene como objetivo principal establecer una gestión automática, centralizada y robusta de la seguridad, garantizando que la infraestructura tecnológica que da soporte a la organización opere bajo condiciones controladas de integridad, confidencialidad y disponibilidad.

Para la correcta aplicación de estas medidas, la metodología se basa en el aprovechamiento de los elementos técnicos nativos del ecosistema Microsoft, articulándose en torno a los siguientes pilares:

- **Uso de Objetos de Directiva de Grupo (GPO):** Se emplearán GPOs como mecanismo principal para el despliegue masivo y homogéneo de configuraciones de seguridad.
- **Gestión de identidad y acceso:** Configuración de políticas en Directorio Activo para garantizar la segregación de roles y funciones, asegurando que los permisos administrativos se asignen bajo el principio de menor privilegio.
- **Alineación normativa base:** Los servidores miembros del dominio deberán haber sido implementados previamente siguiendo las directrices de la guía CCN-STIC-570A25 Perfilado de seguridad para Windows Server (DC o MS).

A continuación, se describe el flujo de trabajo paso a paso para la aplicación de seguridad sobre Internet Information Services de manera centralizada.

ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE INTERNET INFORMATION SERVICES 10 SOBRE WINDOWS SERVER 2025

ANEXO A.1.1. PASO A PASO DE 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".

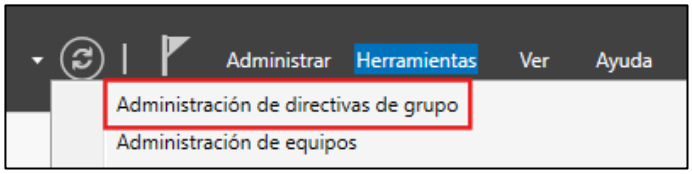


Ilustración 1 - Administración de directivas de grupo

3.	Despliegue en el panel izquierdo hasta llegar a la OU "Domain Controllers".

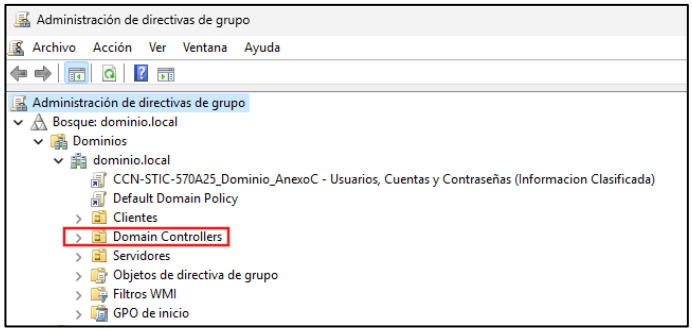


Ilustración 2 - OU Domain Controllers

4.	Despliegue dicha Unidad Organizativa, haga clic derecho sobre el GPO "CCN-STIC-570A25_DC_AnexoA – ADMX (Nivel de Clasificación)", y seleccione "Editar".

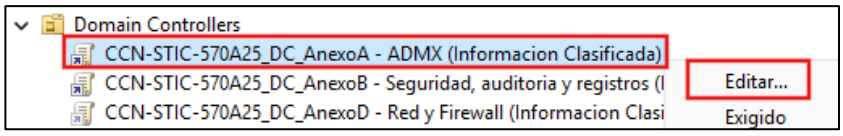


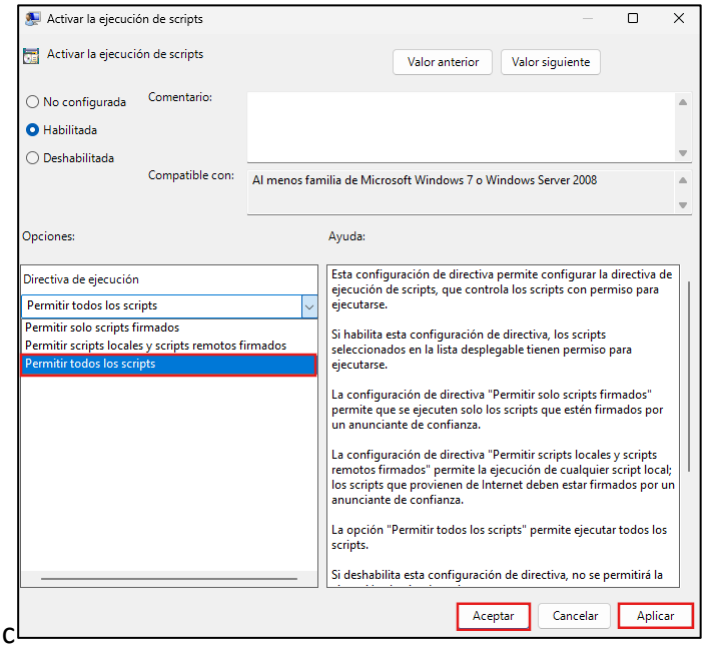
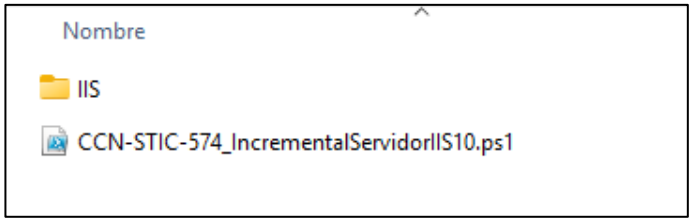
Ilustración 3 - Edición de ADMX 570A25

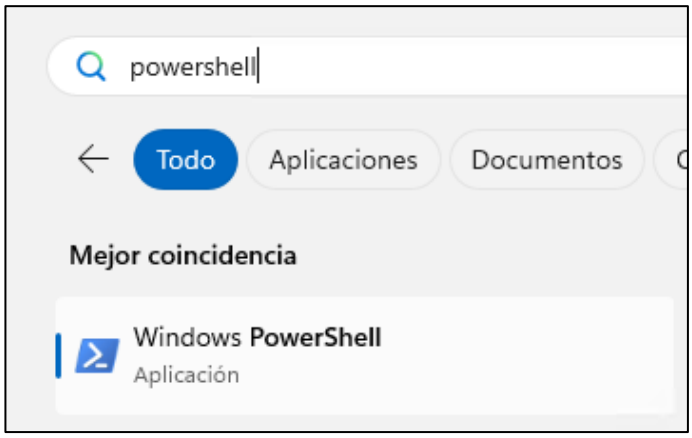
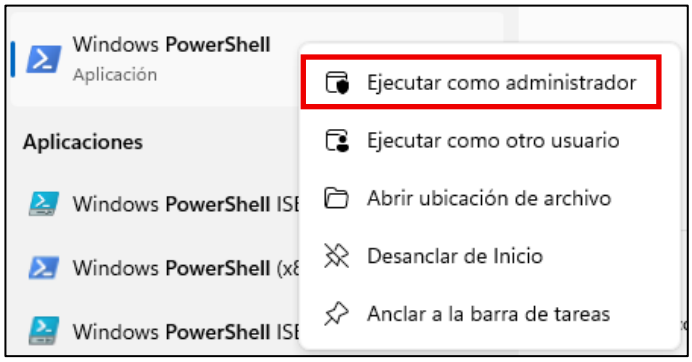
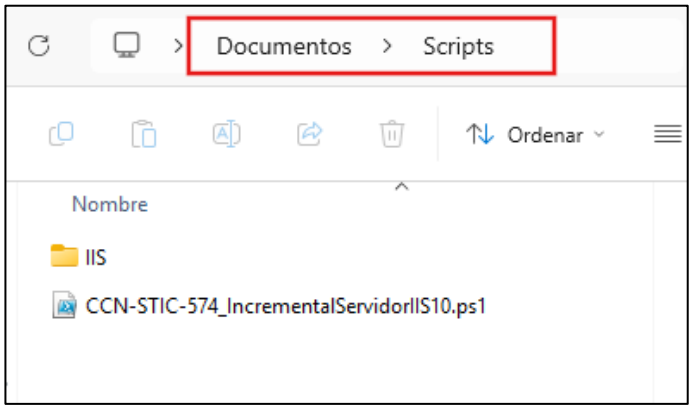
5.	En el panel "Editor de administración de directivas de grupo", despliegue la lista siguiendo la siguiente ruta: "**Configuración del Equipo > Plantillas administrativas > Componentes de Windows > Windows PowerShell**". Haga clic sobre "Windows PowerShell" para consultar las políticas que aplica.

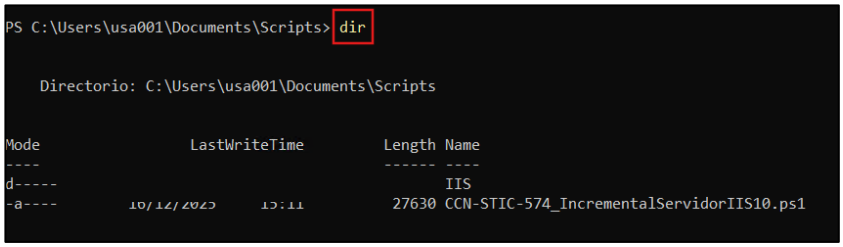
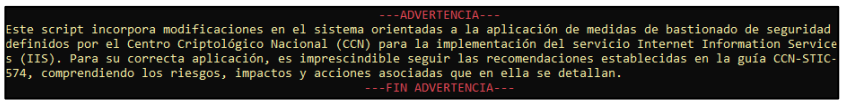
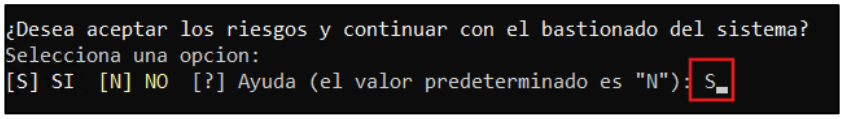
Configuración	Estado	Comentario
Activar registro de módulos	Habilitada	No
Activar el registro de bloque de script de PowerShell	Habilitada	No
Activar la ejecución de scripts	Habilitada	No
Activar la transcripción de PowerShell	Habilitada	No
Establecer la ruta de acceso de origen de Update-Help	No configurada	No

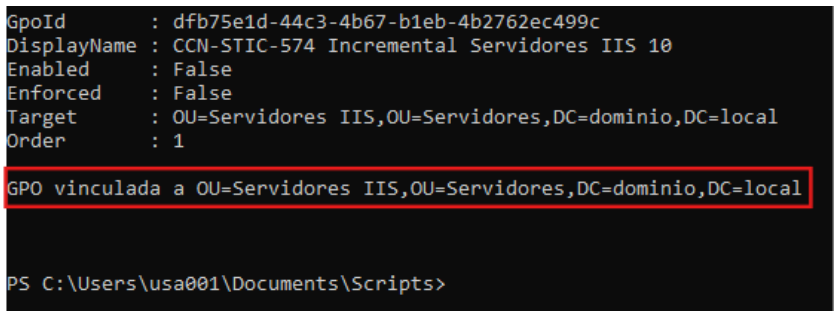
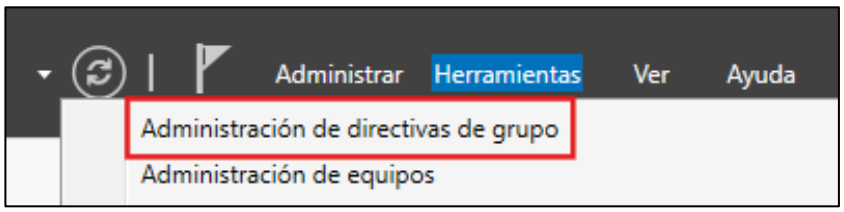
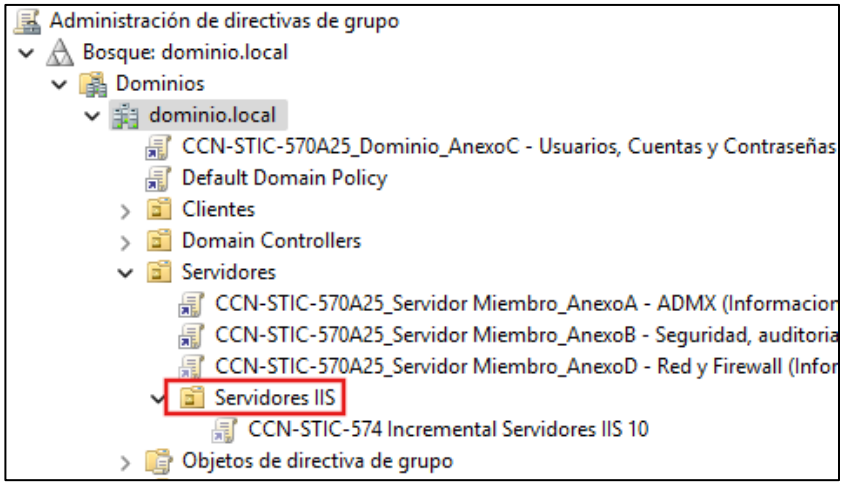
Ilustración 4 - Políticas de PowerShell

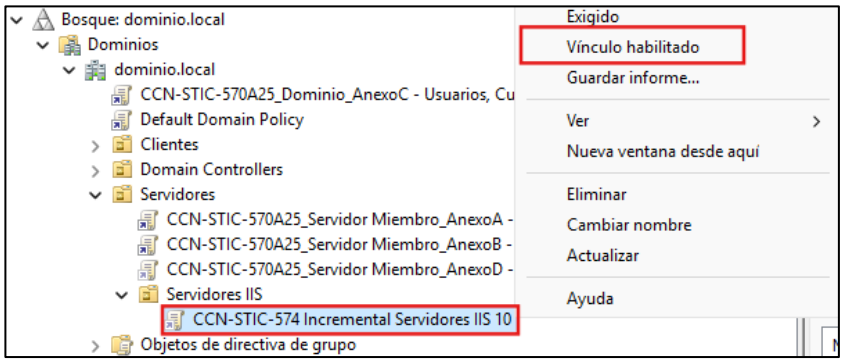
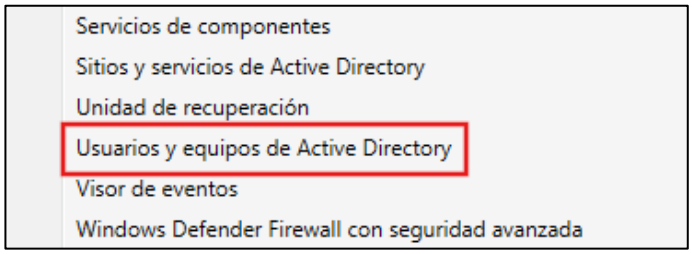
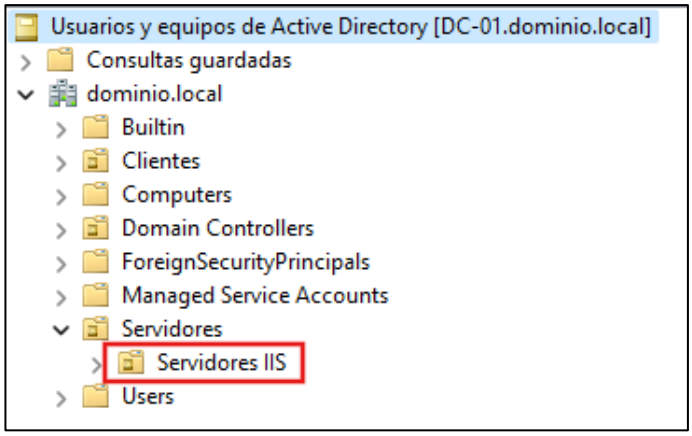
6.	Haga doble clic sobre la política "Activar la ejecución de scripts".

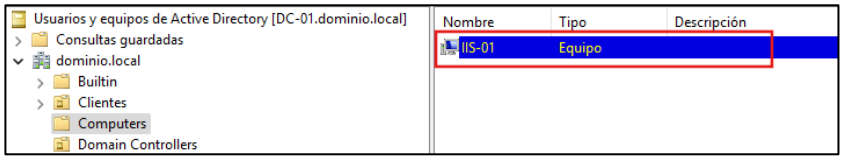
7.	En el desplegable de la política, seleccione “Permitir todos los scripts”, y haga clic en “Aplicar” y “Aceptar”.  *Ilustración 5 - Selección de "Permitir todos los scripts"*
8.	Reinicie el controlador de dominio para que se aplique la configuración correctamente.
9.	Copie los ficheros y directorios que acompañan a esta guía al directorio en la carpeta “Documentos” del usuario administrador. A continuación, descomprima la carpeta. Verifique que en su interior se encuentran los siguientes archivos: - Directorio: IIS - Fichero: CCN-STIC-574_IncrementalServidorIIS10.ps1  *Ilustración 6 - Copia de ficheros necesarios*

10.	Sobre la barra de búsqueda, escriba “PowerShell”:  *Ilustración 7 - Windows PowerShell*
11.	Haga clic derecho, y seleccione “Ejecutar como administrador”:  *Ilustración 8 - Ejecución como administradorr* **Nota:** Si el script no se ejecuta desde PowerShell, existe la posibilidad de que ocurran fallos durante el proceso de copia y/o que no se visualice la información de manera adecuada.
12.	Desde el explorador de archivos, acceda al contenido de carpeta en la que ha copiado los scripts y copie la ruta en el portapapeles con “Ctrl + C”.  *Ilustración 9 - Copia de ruta*

13.	Desde la ventana de PowerShell, utilizando el comando “cd”, acceda a la ruta recientemente copiada.  *Ilustración 10 - Acceso a la ruta*
14.	Ejecute el comando “dir” para verificar la ubicación y el contenido.  *Ilustración 11 - Contenido de la carpeta*
15.	Ejecute el archivo “CCN-STIC-574_IncrementalServicioIIS10.ps1” escribiendo “.\” y pulsando la tecla tabuladora hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución.  *Ilustración 12 - Ejecución del script*
16.	A continuación, se mostrará una advertencia de uso, continuando con el siguiente mensaje:  *Ilustración 13 - Advertencia*
17.	Escribir “S” y pulsar “Enter”.  *Ilustración 14 - Aceptación de advertencia*

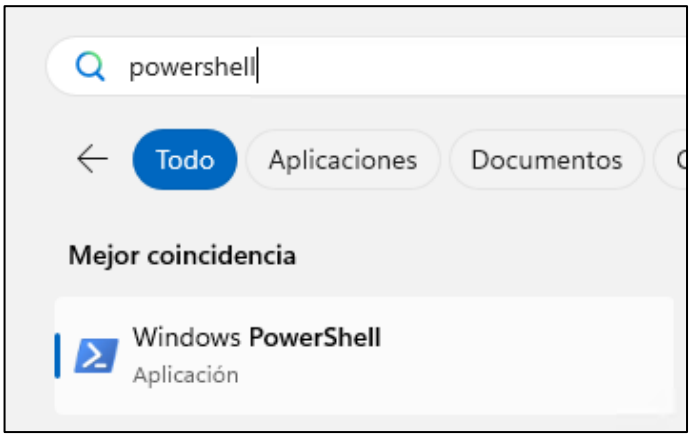
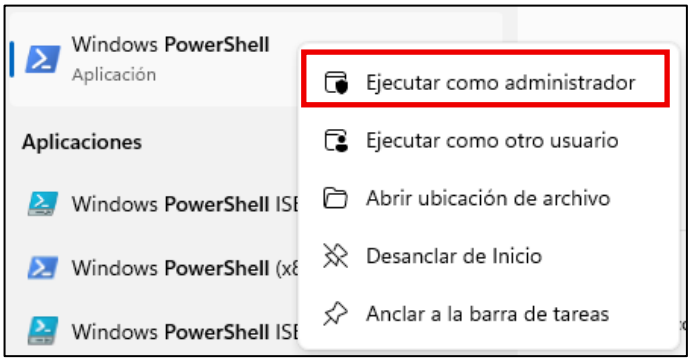
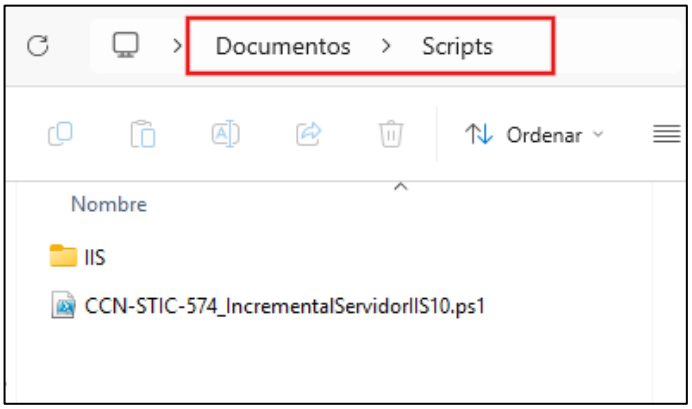
18.	Espere a que finalice la ejecución; al terminar, se mostrará un mensaje indicando que la GPO de IIS se ha vinculado correctamente a la Unidad Organizativa de Servidores IIS.  *Ilustración 15 - GPO vinculada.*
19.	En el "Administrador del servidor", haga clic en "Herramientas" en la barra superior y seleccione "Administración de directivas de grupo".  *Ilustración 16 - Administración de directivas de grupo*
20.	Despliegue la lista del menú izquierdo hasta localizar el dominio y, a continuación, acceda a la Unidad Organizativa de Servidores IIS.  *Ilustración 17 - OU Servidores IIS*

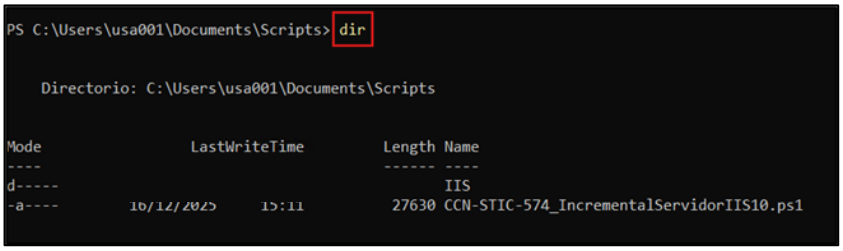
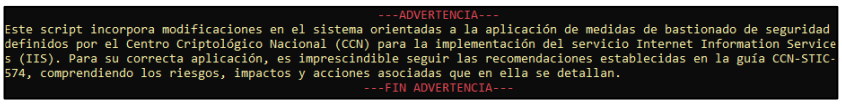
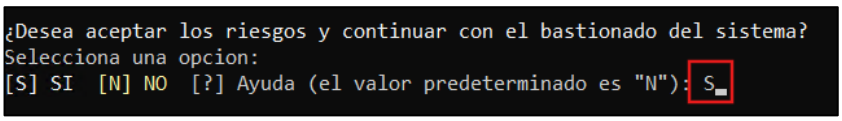
21.	Despliegue dicha OU y haga clic derecho sobre el GPO "CCN-STIC-574 Incremental Servidores IIS 10". Seleccione la opción "Vínculo habilitado".  *Ilustración 18 - Habilitar OU.*
22.	De nuevo en el "Administrador del servidor", haga clic en "Herramientas" en la barra superior, y seleccione "Usuarios y equipos de Active Directory".  *Ilustración 19 - Usuarios y equipos de Active Directory*
23.	Despliegue la lista del panel izquierdo hasta visualizar la OU "Servidores IIS".  *Ilustración 20 - OU Servidores IIS*

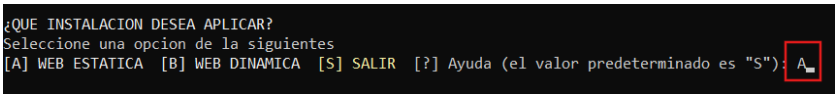
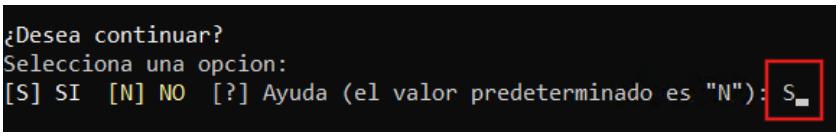
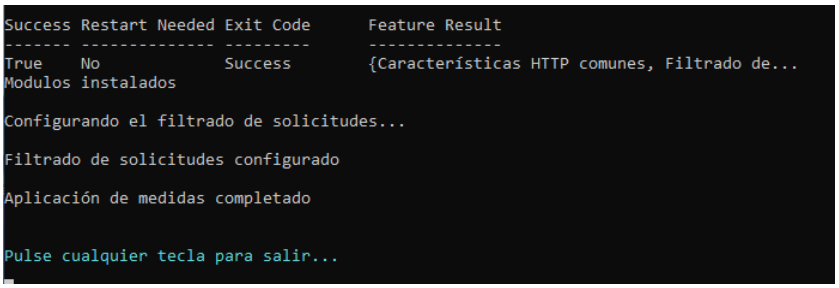
24.	Haga clic sobre la carpeta “Computers” y seleccione el servidor IIS.  *Ilustración 21 - Selección del servidor.*
25.	Arrástrelo a la OU “Servidores IIS”. Aparecerá una advertencia. Haga clic en “Sí”.
26.	A continuación, reinicie uno a uno los controladores de dominio para que se les aplique el GPO de Dominio. Una vez hecho, reinicie el servidor IIS para que se les apliquen los GPOs de Dominio de Servidor.

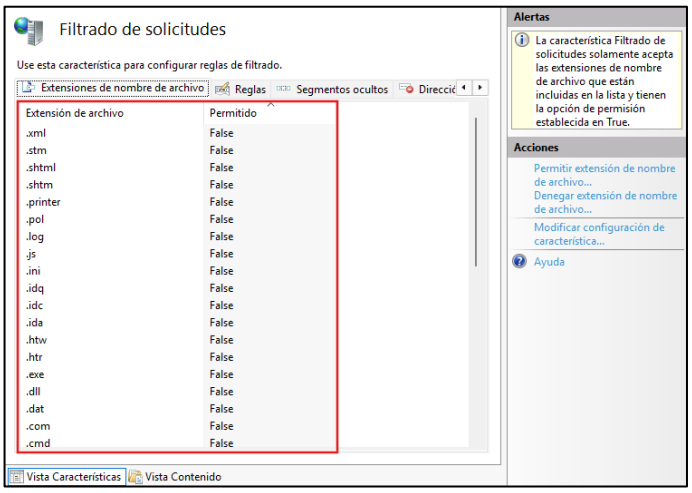
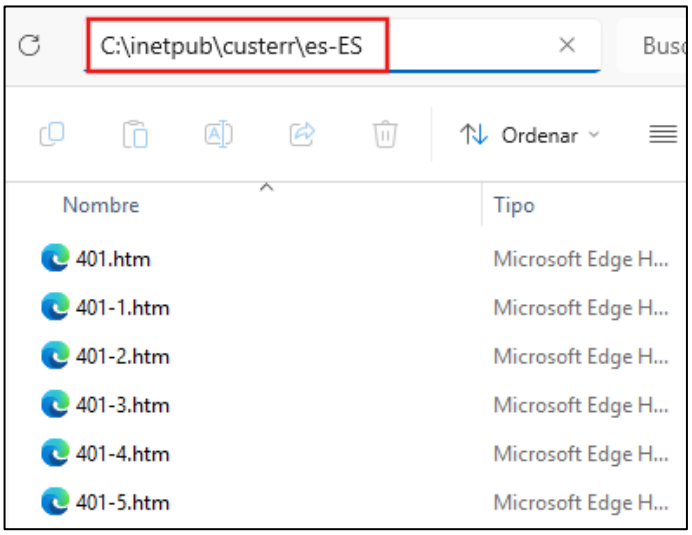
ANEXO A.1.2. PASO A PASO DE CONFIGURACIÓN DE SEGURIDAD EN SERVIDOR WEB ESTÁTICO

Paso	Descripción
1.	Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en el Servidor IIS.
2.	Copie los ficheros y directorios que acompañan a esta guía al directorio en la carpeta “**Documentos**” del usuario administrador. A continuación, descomprima la carpeta. Verifique que en su interior se encuentran los siguientes archivos: - Directorio: IIS - Fichero: CCN-STIC-574_IncrementalServidorIIS10.ps1  *Ilustración 22 - Copia de ficheros necesarios*

3.	Sobre la barra de búsqueda, escriba “PowerShell”:  *Ilustración 23 - Windows PowerShell*
4.	Haga clic derecho, y seleccione “Ejecutar como administrador”:  *Ilustración 24 - 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.
5.	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 25 - Copia de ruta*

6.	Desde la ventana de PowerShell, utilizando el comando “cd”, acceda a la ruta recientemente copiada.  *Ilustración 26 - Acceso a la ruta*
7.	Ejecute el comando “dir” para verificar la ubicación y el contenido.  *Ilustración 27 - Contenido de la carpeta*
8.	Ejecute el archivo “CCN-STIC-574_IncrementalServicioIIS10.ps1” escribiendo “.\” y pulsando la tecla tabuladora hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución.  *Ilustración 28 - Ejecución del script*
9.	A continuación, se mostrará una advertencia de uso, continuando con el siguiente mensaje:  *Ilustración 29 - Advertencia*
10.	Escribir “S” y pulsar “Enter”.  *Ilustración 30 - Aceptación de advertencia*

11.	Aparecerán dos opciones de configuración: - [A] Web Estática - [B] Web Dinámica Escribir “A” y continuar con la configuración del servidor.  *Ilustración 31 - Opciones de instalación*
12.	Espere a que termine la ejecución. Una vez hecho, deberá escribir “S” y pulsar “Enter” para continuar con la configuración.  *Ilustración 32 - Continuar*
13.	Una vez haya terminado, pulsar cualquier tecla para salir.  *Ilustración 33 - Finalización del script*

14.	Se habrá incorporado el "filtrado de solicitudes" del entorno de administración. Acceda y revise todas las pestañas para comprobar que "Extensiones de nombre de archivo" incorpora un listado con todos los valores no permitidos, figuran como "False", y "Segmentos ocultos" tiene varias entradas, entre ellas web.config. **"Menú inicio > Herramientas administrativas > Administrador de Internet Information Services (IIS) > [nombre_del_servidor] > Filtrado de solicitudes".**  *Ilustración 34 - Filtrado de solicitudes*
15.	Verifique que la carpeta **"C:\Inetpub\custerr\es-ES\"** existe, ya que se utilizará para evitar mostrar información adicional a posibles atacantes mediante mensajes de error detallados.  *Ilustración 35 - Carpeta de mensajes de error* **Nota**: la ruta será diferente si se ha especificado otro volumen en el entorno.

16. En dicha carpeta debe alojar el archivo **"error.htm"**, incluido en el directorio **"IIS"** dentro de la carpeta de la guía. Este archivo será el mensaje de error estándar que se mostrará independientemente de la causa que lo genere.

Ilustración 36 - Archivo error.htm

17. Los permisos locales (permisos NTFS) de la carpeta **"C:\Inetpub\custerr"** estarán asignados como los que se muestran en la siguiente tabla, de no ser así, en su servidor, deberá hacer los cambios necesarios.

Carpeta	Grupo/Usuario	Permiso NTFS
C:\Inetpub\custerr	CREATOR OWNER	Permiso especial: Control total solo esta subcarpeta y archivos
	SYSTEM	Control total
	Administradores	Control total
	Usuarios	Lectura y Ejecución
	TrustedInstaller	Control total

18. Sobre la barra de búsqueda, escriba "Administrador de Internet Information Services (IIS)".

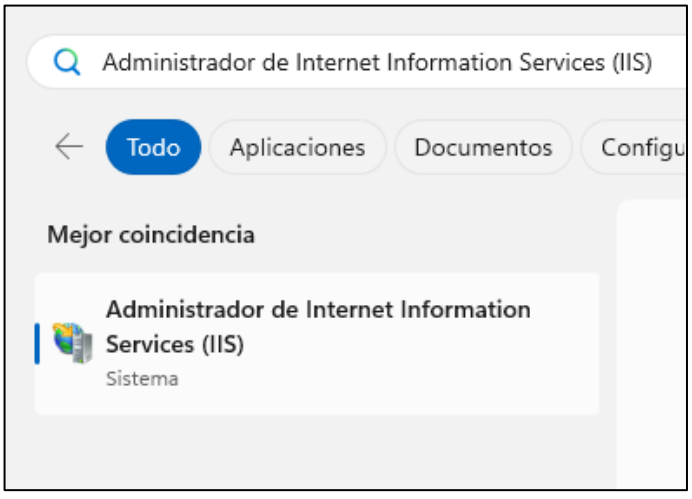


Ilustración 37 - Administrador de Internet Information Sevices

19.	Haga clic derecho y seleccione “Ejecutar como administrador”.
20.	En el árbol de conexiones, sitúese sobre el nodo “**Administrador de Internet Information Services (IIS) > [nombre_del_servidor]**”.

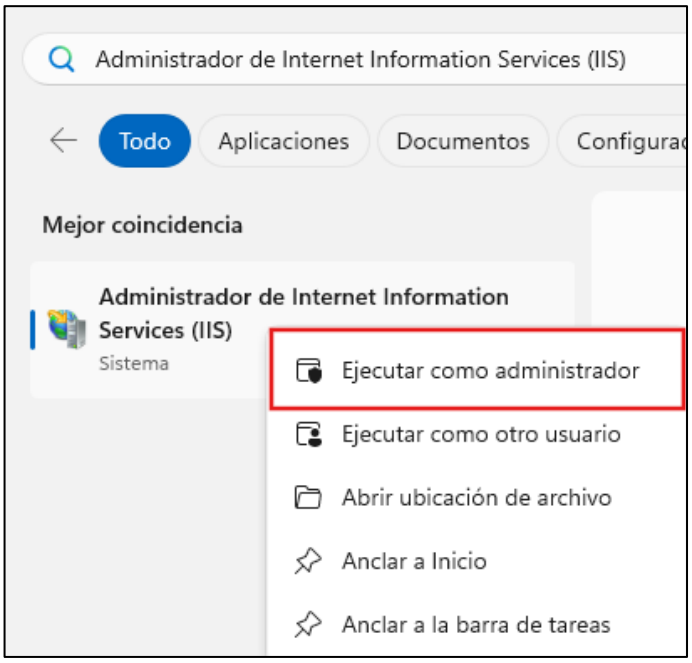


Ilustración 38 - Ejecutar como administrador

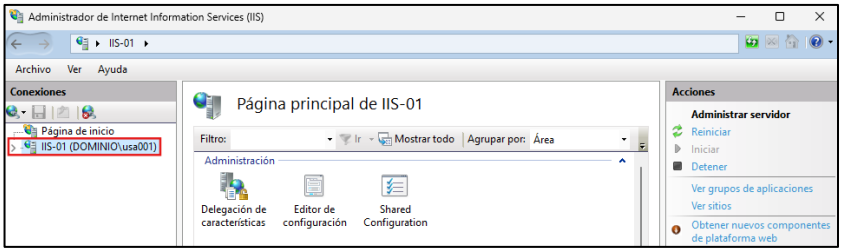
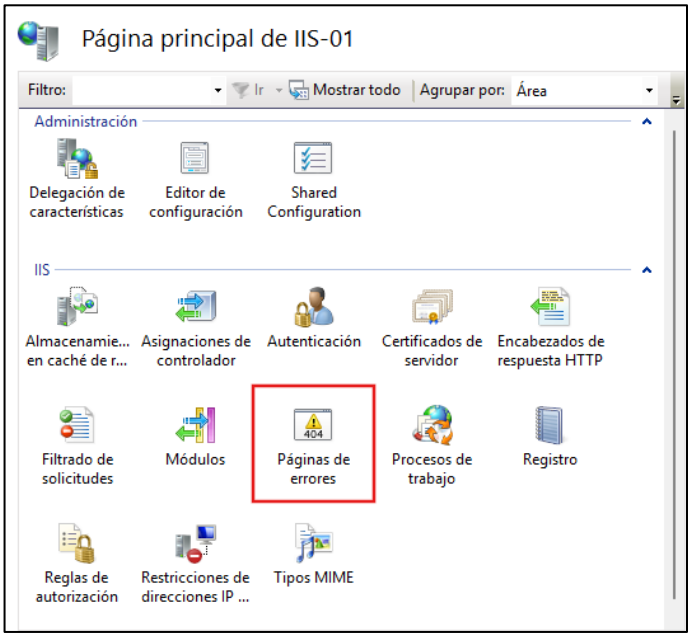
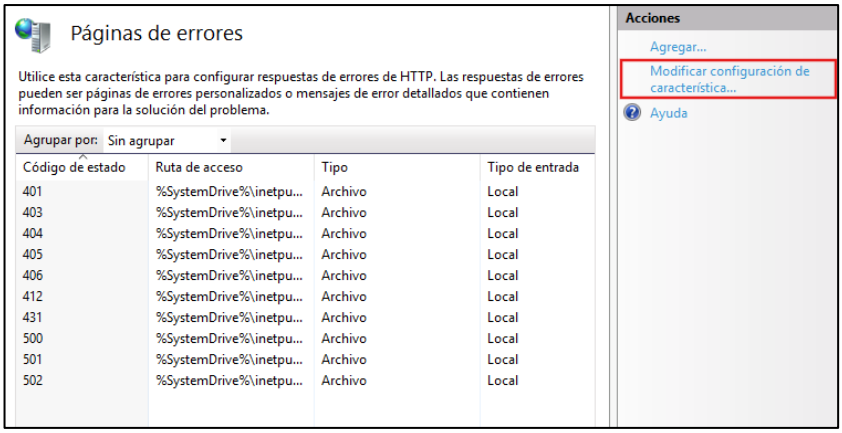
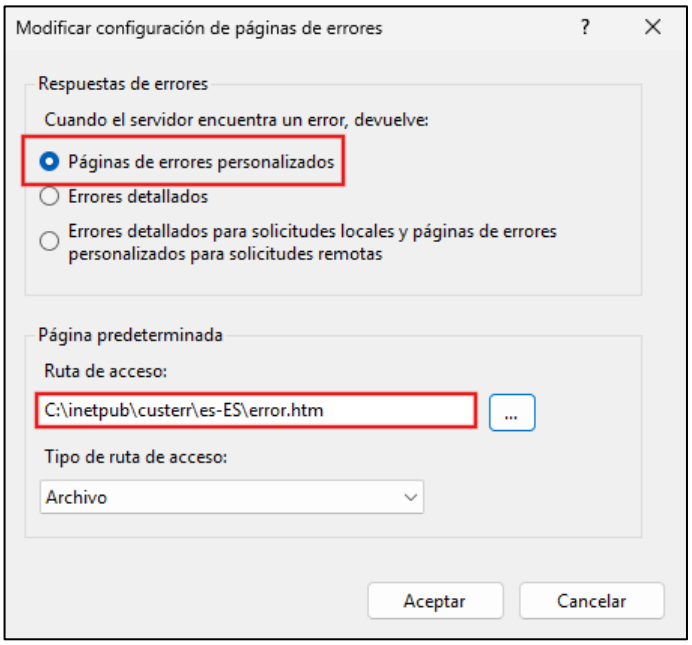
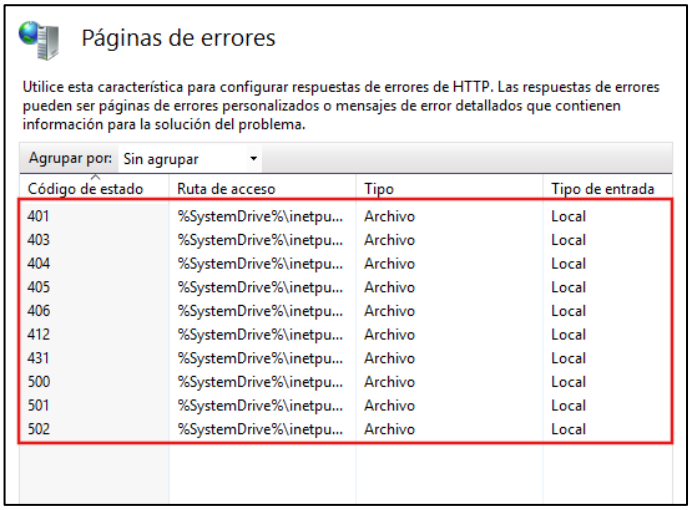
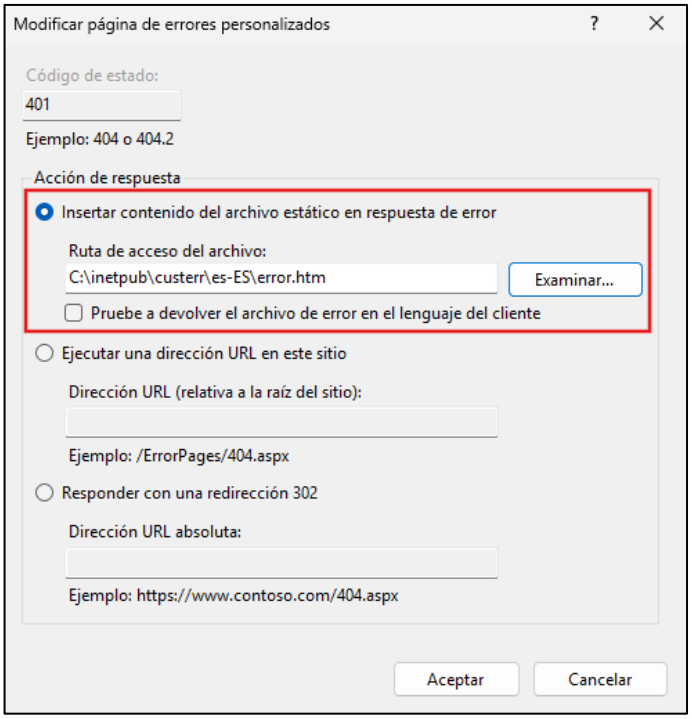
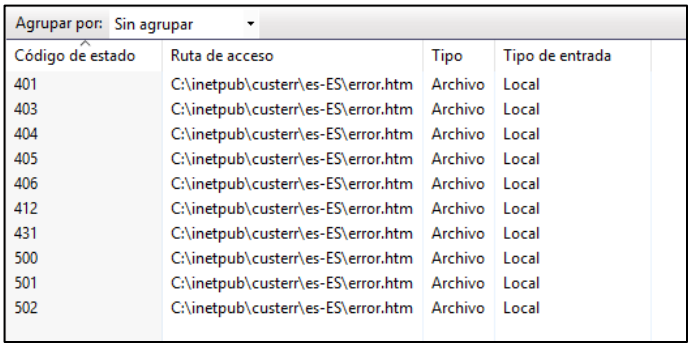
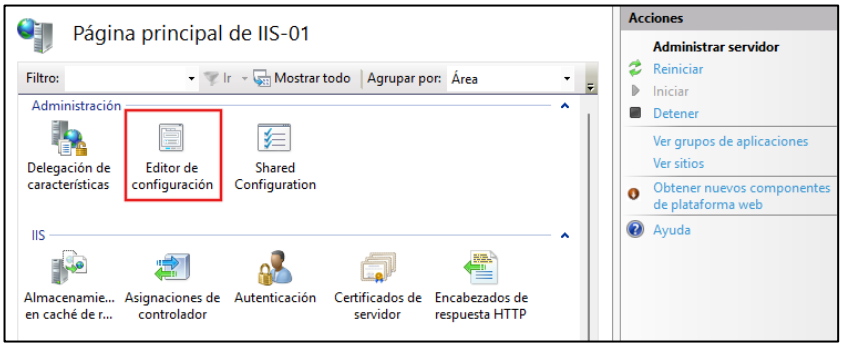
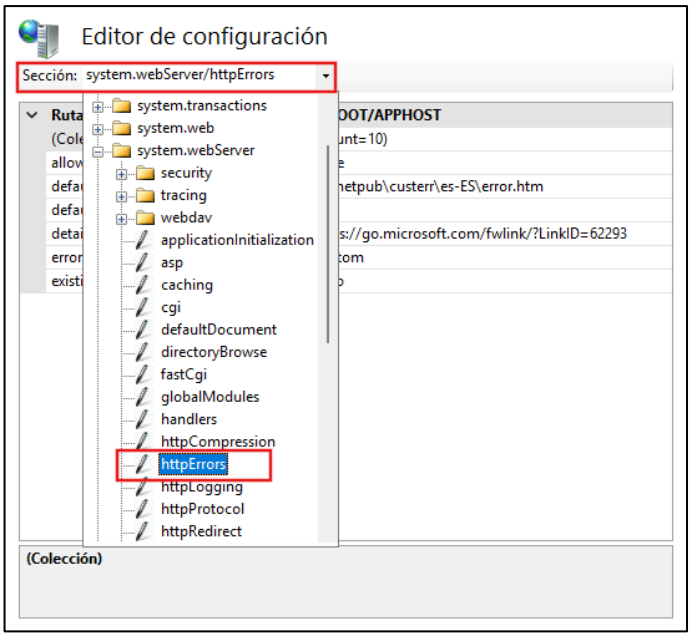


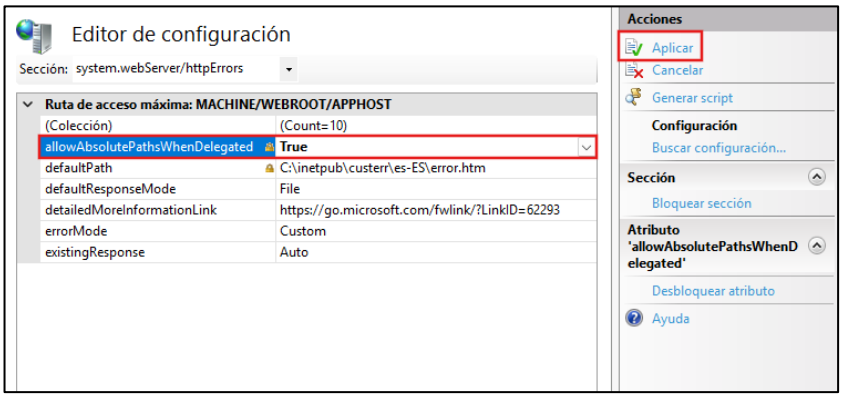
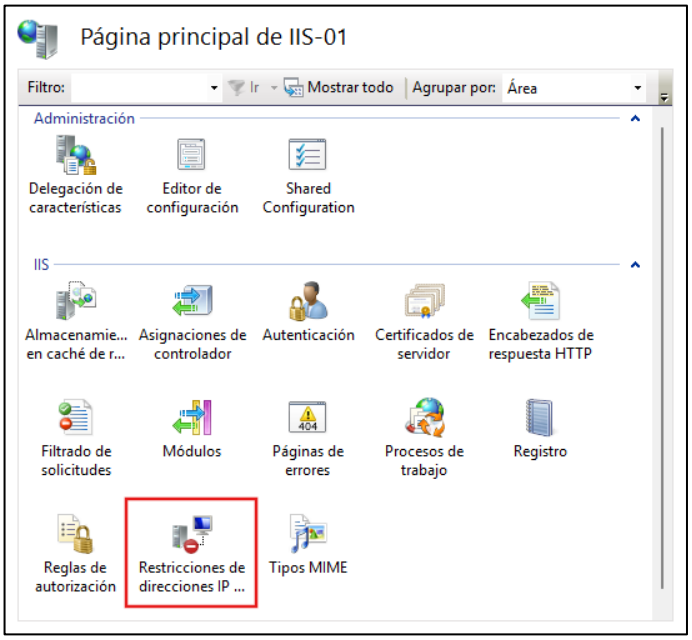
Ilustración 39 - Página principal de IIS

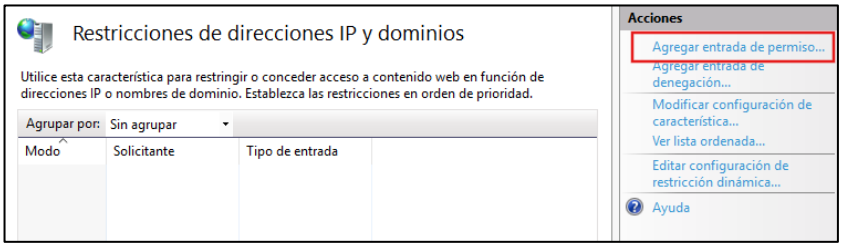
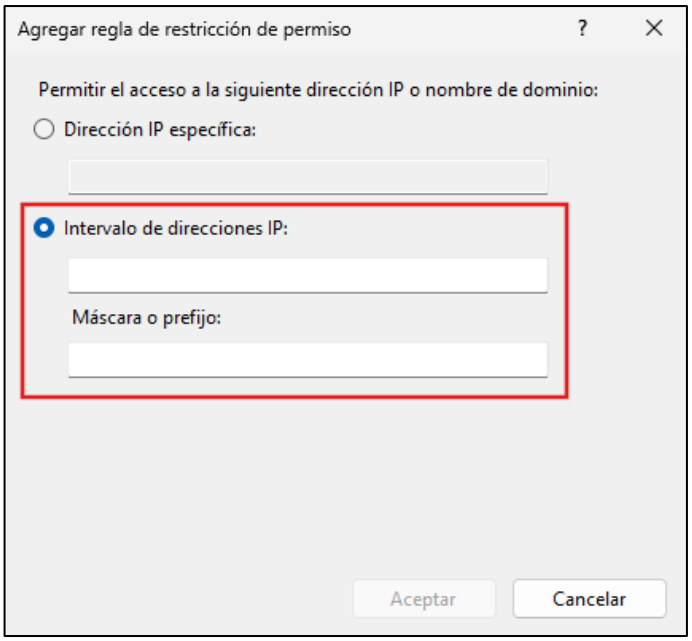
21.	Seleccione “Páginas de errores” en el menú central.  *Ilustración 40 - Página de errores*
22.	Una vez abierta la característica, seleccione en el menú “Acciones”, en el lateral derecho, “Modificar configuración de característica…”.  *Ilustración 41 - Modificar página de errores*

23.	Ahora elija el fichero copiado en pasos anteriores, "error.htm", como error personalizado por defecto. Pulse "Aceptar" para completar la configuración.  *Ilustración 42 - Configuración de página de errores*
24.	Para la personalización de los errores, y evitar que muestren información que podría ayudar a posibles atacantes a crear un perfil de sus sistemas, termine la personalización de todos los errores que se muestran en la lista de página de errores.  *Ilustración 43 - Códigos de errores*

25.	Para cada código de estado, seleccione la línea y haga clic en “Modificar…” en el menú “Acciones”. Configure los errores con los valores indicados a continuación. - Seleccione “Insertar contenido del archivo estático en respuesta de error”. - Desmarque “Pruebe a devolver el archivo de error en el lenguaje del cliente”. - Ruta de acceso del archivo: C:\inetpub\custerr\es-ES\error.htm Pulse sobre “Aceptar” para finalizar la configuración.  *Ilustración 44 - Modificación de códigos de errores*
26.	Cuando termine se mostrará la ventana de errores siguiente.  *Ilustración 45 - Ventana de errores configurada*

27.	Edite el archivo applicationHost.config para habilitar el uso de rutas absolutas. Vuelva a situarse sobre el servidor y seleccione **"Editor de configuración". "Menú inicio > Herramientas administrativas > Administrador de Internet Information Services (IIS) > [nombre_del_servidor] > Editor de configuración".**  *Ilustración 46 - Editor de configuración*
28.	En la lista desplegable "Sección" marque "system.webServer/httpErrors".  *Ilustración 47 - httpErrors*

29.	Cuando se abra la ventana cambie la variable “allowAbsolutePathsWhenDelegated” a “True” y seleccione “Aplicar” en el menú” Acciones”.  *Ilustración 48 - allowAbsolutePathsWhenDelegated en "True"*
30.	Ahora va a limitar el acceso al servidor según las direcciones IP de su red. Vuelva a la página principal del servidor IIS.
31.	Acceda a la funcionalidad “Restricciones de direcciones IP y dominios”. **“Administrador de Internet Information Services (IIS) > [nombre_del_servidor] > Restricciones de direcciones IP y dominios”**  *Ilustración 49 - Restricciones de direcciones IP*

32.	Se abrirá una ventana sin ninguna regla creada, por lo que debe incluir las redes que tendrán acceso al servidor. Para ello, seleccione la opción "Agregar entrada de permiso…" en el panel "Acciones".  *Ilustración 50 - Agregar entrada de permiso*
33.	Introduzca el rango de direcciones IP correspondiente a su red LAN. En el ejemplo se supone que el servidor se encuentra en ese intervalo.  *Ilustración 51 - Intervalo de direcciones IP* **Nota:** La red que se ha incluido es la propia del ejemplo, es indispensable que adapte este paso a su entorno. Si no conoce la red o subred donde se alojan los equipos consulte con su administrador de redes. Su entorno podría incluir más de una subred, puede agregar cuantas reglas como sean necesarias.

34.	Ahora va a configurar la autenticación a utilizar en su entorno. Acceda a la herramienta de administración de IIS, sección "Autenticación". **"Menú inicio > Herramientas administrativas > Administrador de Internet Information Services (IIS) > [nombre_del_servidor] > Autenticación"**

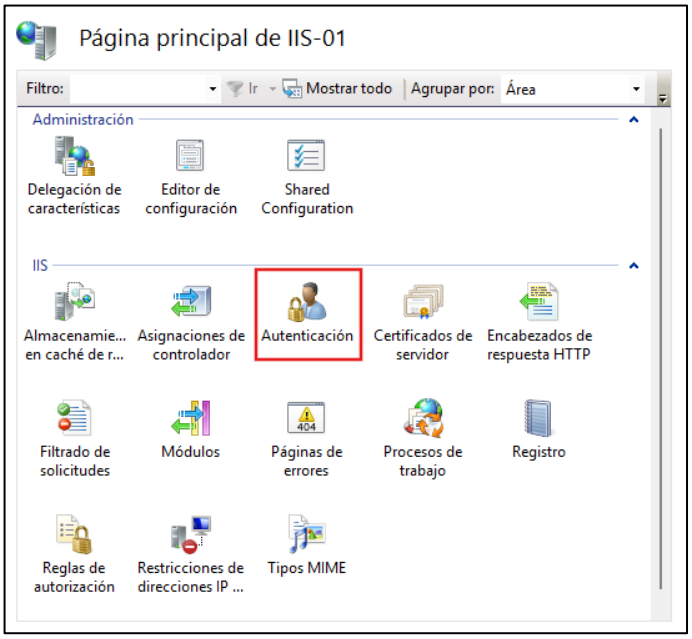


Ilustración 52 - Autenticación

35.	Proceda a habilitar el método "Autenticación de Windows" para que esté operativo. Seleccione "Autenticación de Windows" y en el panel "Acciones" pulse sobre "Habilitar".

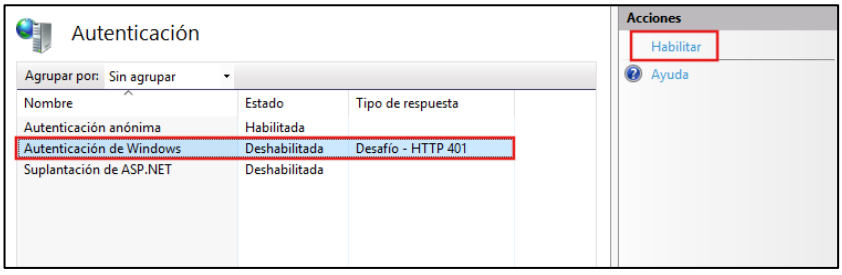


Ilustración 53 - Habilitar autenticación de Windows

36.	Intentando minimizar el riesgo, si todos sus clientes están autenticados por el dominio y acceden a este servidor por la red LAN, debería deshabilitar la autenticación anónima. Para ello seleccione "Autenticación anónima" y "Deshabilitar".

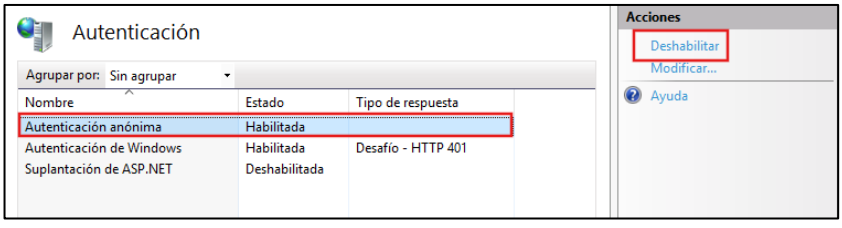
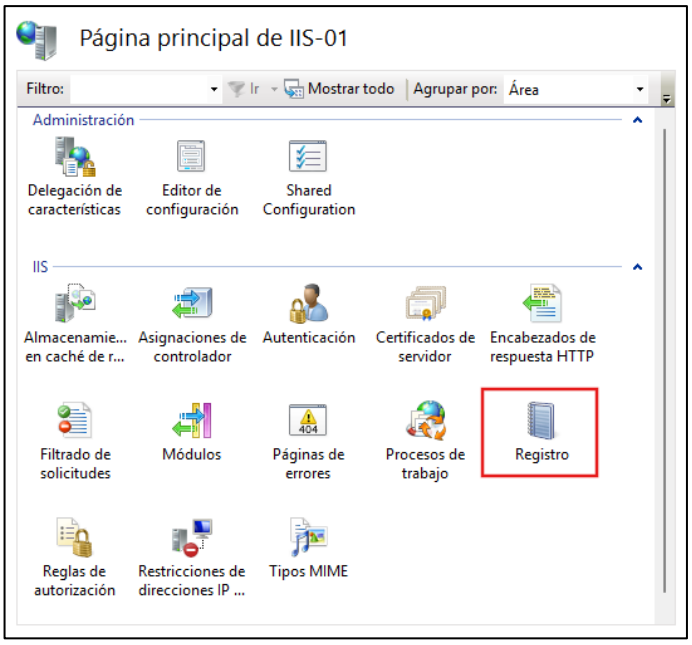
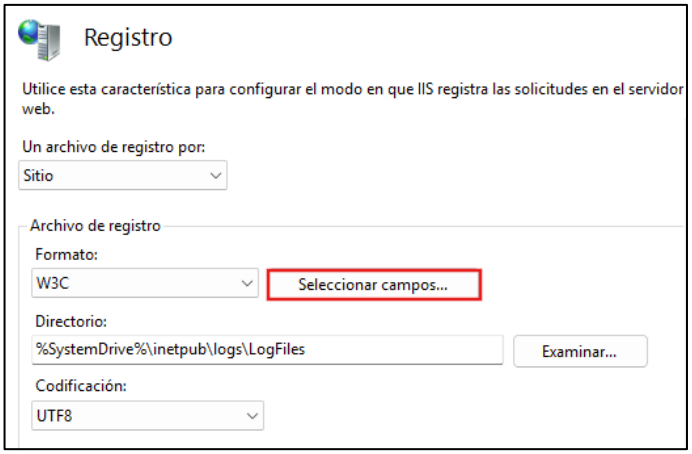
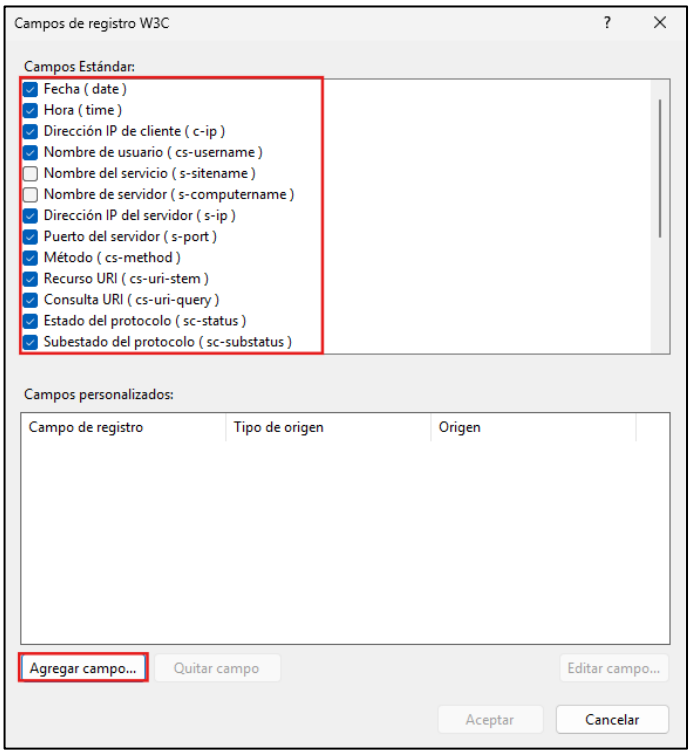
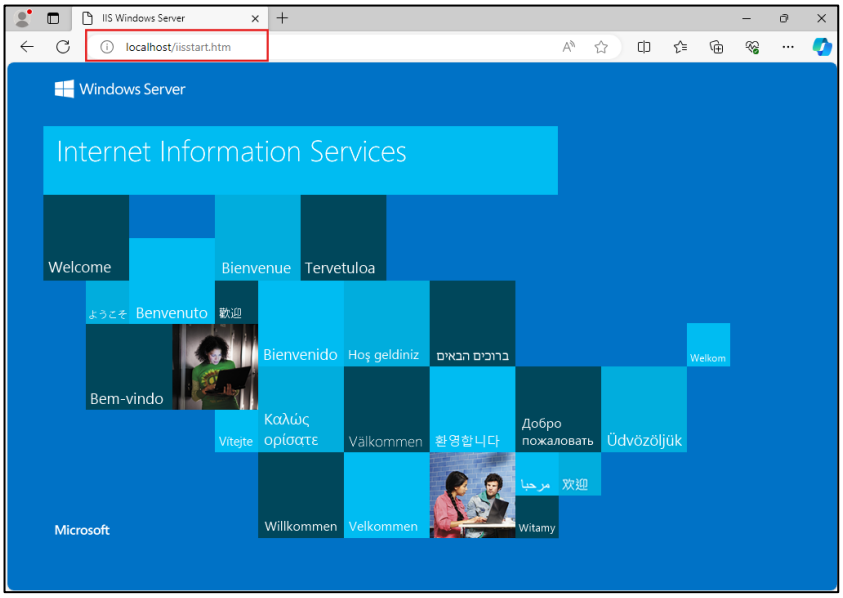


Ilustración 54 - Deshabilitar autenticación anónima

37.	En los siguientes pasos va a comprobar que la configuración de los registros es la adecuada para su entorno. Este seguimiento es indispensable para poder asegurar el servidor ya que de otra forma sería imposible realizar un análisis forense, por ejemplo, después de un ataque o robo de información.
38.	Acceda a la herramienta de administración de IIS, sección "Registro". **"Menú inicio > Herramientas administrativas > Administrador de Internet Information Services (IIS) > [nombre_del_servidor] > Registro".**  *Ilustración 55 - Registro*
39.	El registro queda habilitado con los valores por defecto después de la instalación. Haga clic en "Seleccionar campos…" para personalizar el registro.  *Ilustración 56 - Campos de registro*

40.	Compruebe qué campos se recogerán en el fichero de registro y asegúrese que coincide con las necesidades del entorno. Los valores marcados por defecto suelen ser suficientes, pero no descarte marcar otros.  *Ilustración 57 - Comprobación de campos* **Nota:** Existe la posibilidad de incluir en esta ventana campos personalizados.
41.	A continuación, asegurará los ficheros de logs contra posibles intrusiones, borrados, alteraciones, etc. **Nota:** Recuerde que su unidad puede ser distinta a la original “C:\”.

42.	Para conseguir que se cree la carpeta donde se van a alojar las subcarpetas de registro de cada sitio web, "**C:\inetpub\logs\logfiles**", es necesario generar, al menos un acceso. Para ello, abra Microsoft Edge desde el Menú inicio del servidor IIS y acceda a la URL http://localhost/iisstart.htm  *Ilustración 58 - URL inicial*
43.	En los pasos siguientes se le detalla cómo configurar los permisos locales, permisos NTFS, de la carpeta "**C:\inetpub\logs\logfiles**", que deben quedar como los que se muestran en la siguiente tabla.

Carpeta	Grupo/Usuario	Permiso NTFS
C:\inetpub\logs\logfiles	CREATOR OWNER	Permiso especial: Control total solo esta subcarpeta y archivos
	SYSTEM	Control total
	Administradores	Control total
	Auditores	Leer
	TrustedInstaller	Control total

44.	Abra el Explorador de archivos y diríjase a la carpeta "**C:\inetpub\"**, con el botón derecho, sobre la carpeta **logs**, selecciones "Propiedades".

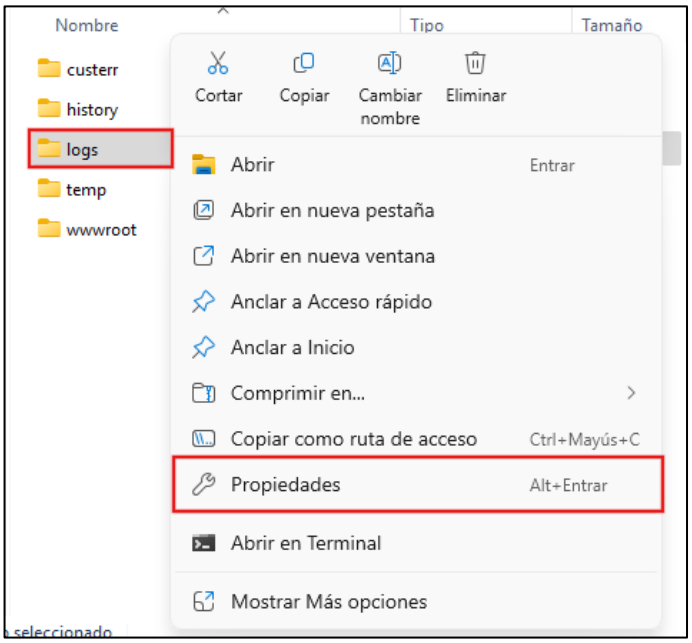


Ilustración 59 - Propiedades de logs

45.	Sitúese en la pestaña “Seguridad”, donde observa que la carpeta tiene permisos aplicados directamente. Presiones “Editar” para modificar los permisos.

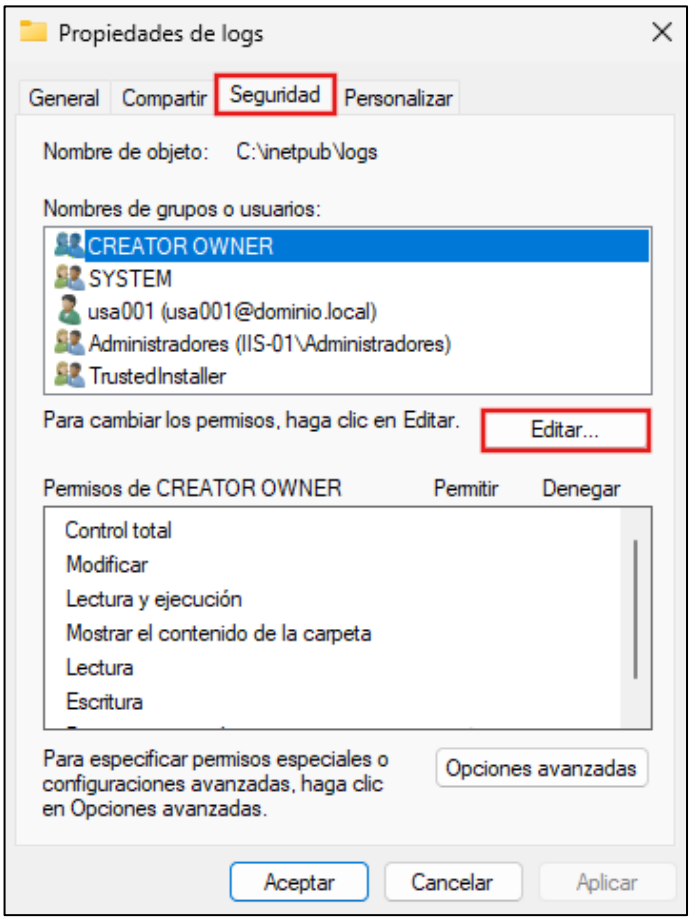
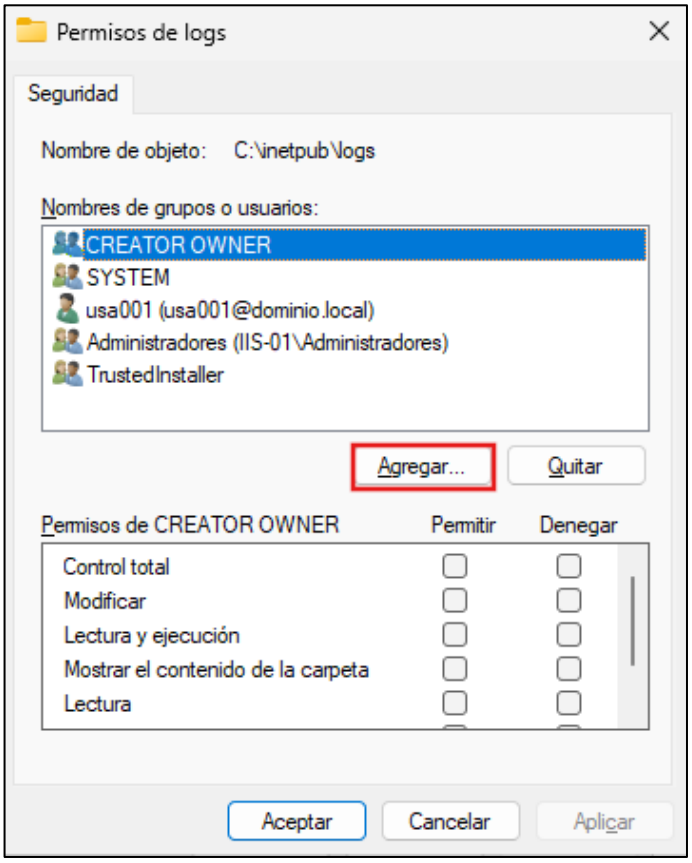
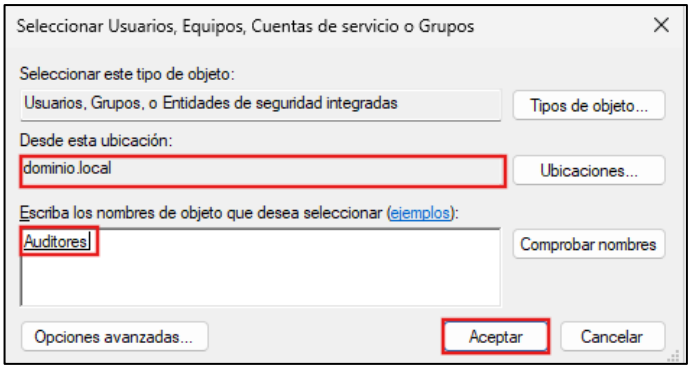
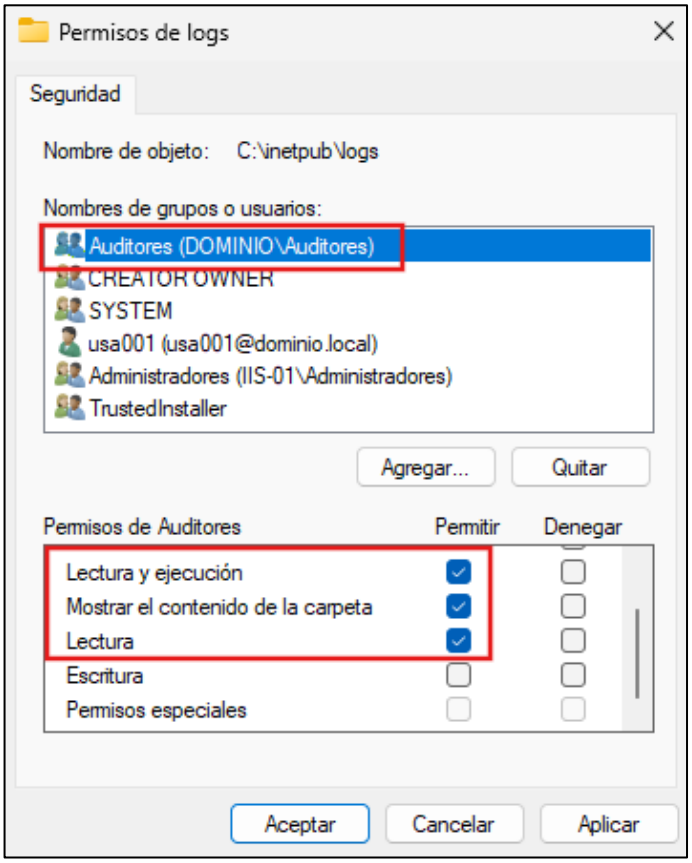
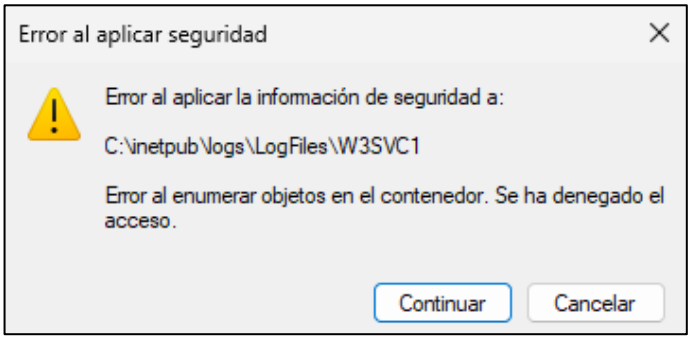
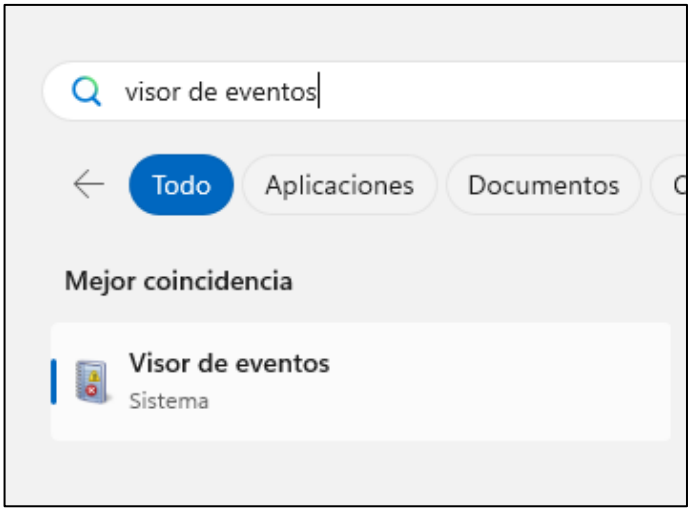
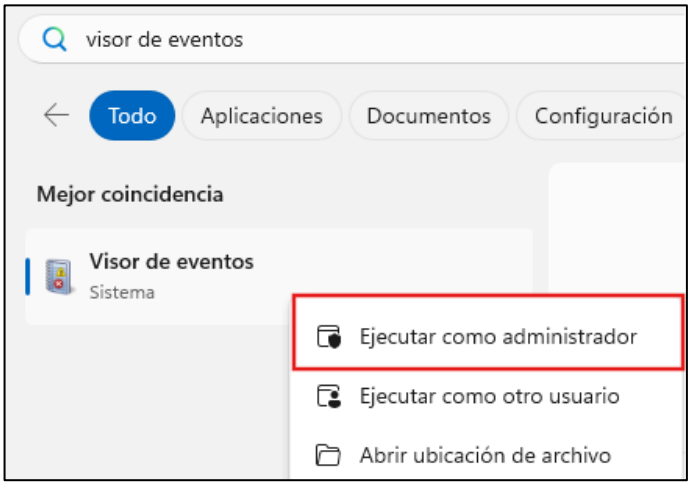


Ilustración 60 - Pestaña de seguridad

46.	Presione el botón “Agregar…”, para en los siguientes pasos añadir el grupo “Auditores”.  *Ilustración 61 - Agregar permisos*
47.	Escriba “Auditores” y acepte para que se añada.  *Ilustración 62 - Agregar grupo de Auditores* **Nota:** Existe la posibilidad de que el grupo “Auditores” no exista de forma predeterminada en el dominio. En ese caso, cree el grupo en un servidor Controlador de Dominio o seleccione un grupo que sea el encargado de llevar a cabo la tarea de Auditores.

48.	Los permisos que se adjudican por defecto, para los “Auditores” son los siguientes.  *Ilustración 63 - Permisos de auditores*
49.	En algunas circunstancias, se le puede mostrar un mensaje como el siguiente, ya que los permisos de la carpeta **“C:\inetpub\logs\”** están marcados para ser actualizados por herencia, recibirán los nuevos permisos automáticamente. Presione “Continuar” para conseguir aplicar los cambios  *Ilustración 64 - Mensaje de aviso* **Nota:** El aviso le indica que los cambios no se aplicarán sobre la carpeta” W3SVC1” y los ficheros que contenga. La carpeta es la propia del registro del Default Web Site. Para cada sitio web alojado en el servidor se creará una carpeta específica que se alojará en el mismo camino que la del Defaul Web Site.

50.	En los siguientes pasos va a activar la auditoría del servidor. En este caso se permitirá registrar acciones sobre los servicios y no de acceso de usuarios, como en el “Registro”, configurado en pasos anteriores.
51.	Sobre la barra de búsqueda, escriba “Visor de eventos”.  *Ilustración 65 - Visor de eventos*
52.	Haga clic derecho y seleccione “Ejecutar como administrador”.  *Ilustración 66 - Ejecutar modo administrador*

53.	Despliegue el siguiente nodo. **"Visor de eventos (local) > Registro de aplicaciones y servicios > Microsoft > Windows > IIS-Configuration".**

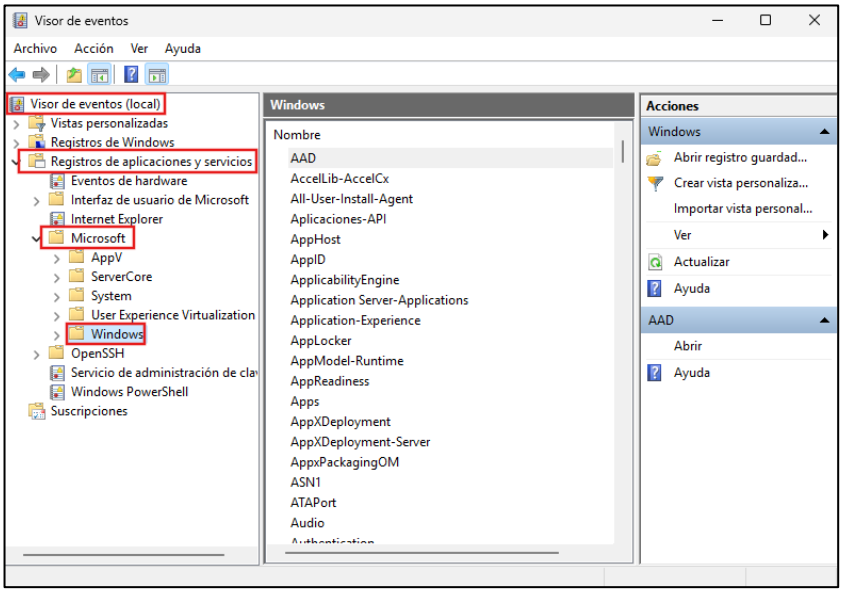


Ilustración 67 - Carpeta del visor de eventos

54.	Windows Server 2025 dispone de dos grupos de registros para IIS, dentro del nodo de configuración se encuentran el registro administrativo y el registro operativo. Es necesario activar ambos.

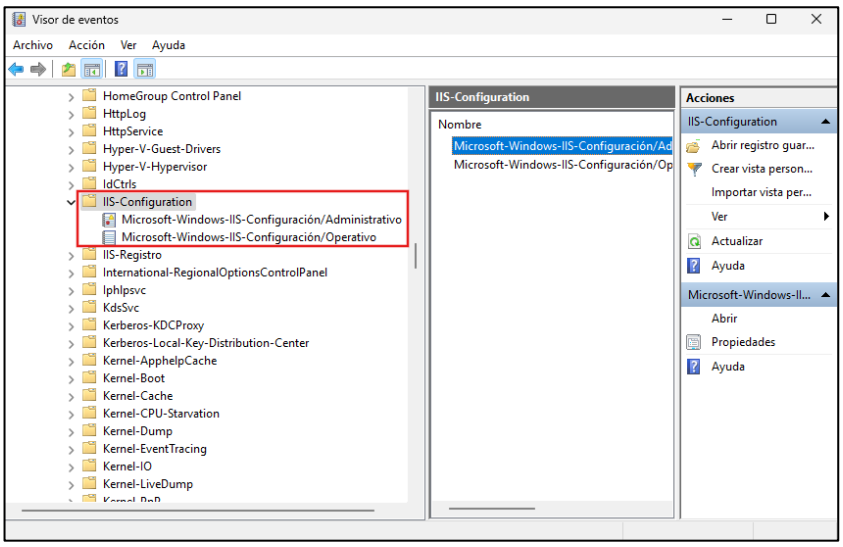


Ilustración 68 - Registros

55.	Sitúese sobre el registro “Administrativo”, abra el menú contextual con el botón derecho del ratón y seleccione “Habilitar registro”.

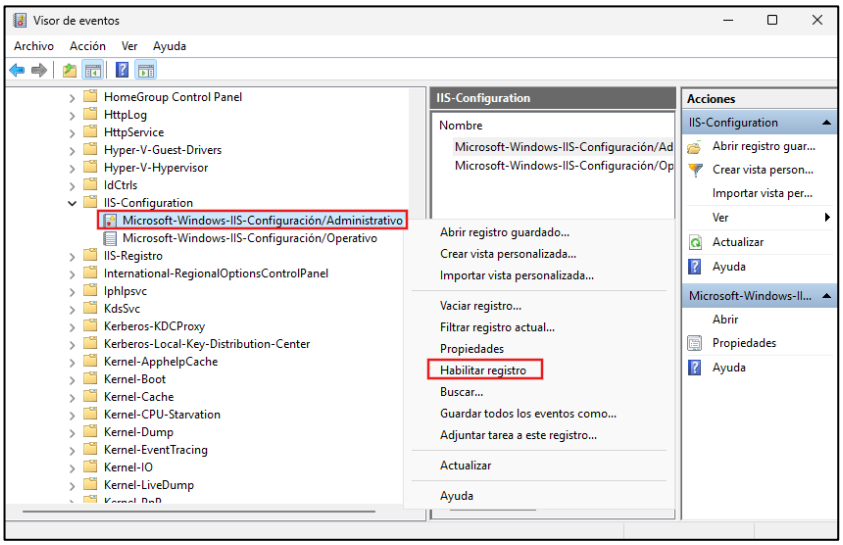


Ilustración 69 - Habilitar registro administrativo

56.	Haga lo mismo para el registro “Operativo.”

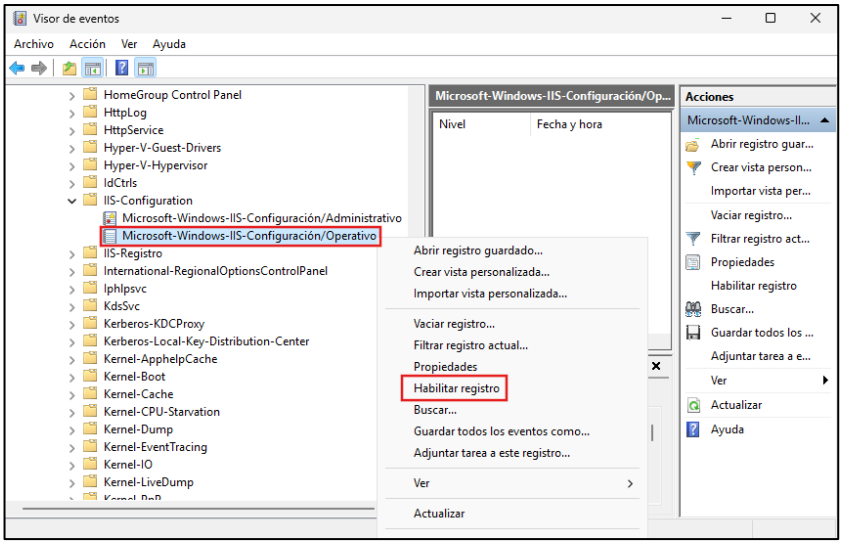
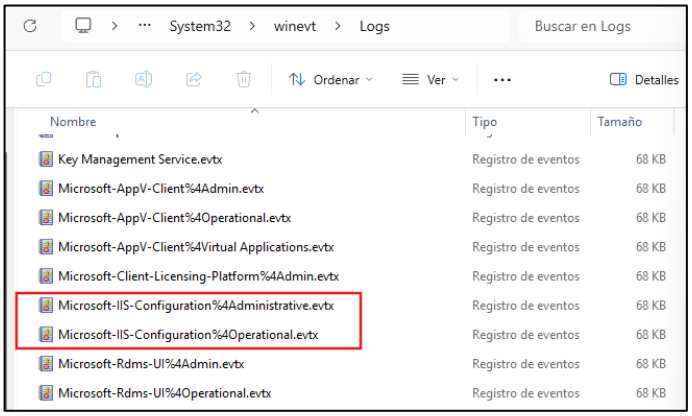
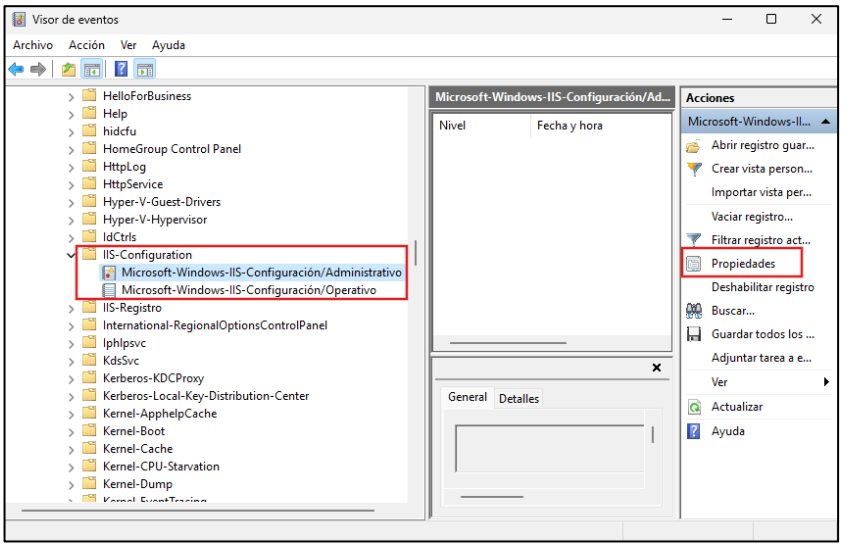
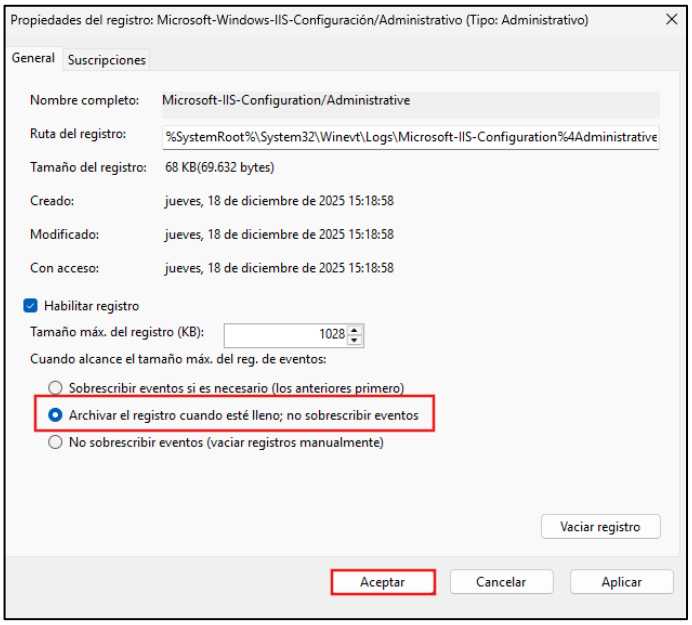


Ilustración 70 - Habilitar registro operativo

Cualquier acción operativa y administrativa realizada sobre el servidor quedará recogida a partir de ahora.

57.	Los registros se habrán creado en el disco duro, en la partición del sistema operativo (habitualmente en "C:\") en la ruta **"%SystemRoot%\System32\winevt\Logs"**, con los nombres: Microsoft IIS-Configuration%4Operational.evtx y Microsoft IIS-Configuration%4Administrative.evtx.  *Ilustración 71 - Registros creados*
58.	Para acceder a las propiedades de los ficheros, seleccione un fichero y pulse sobre la opción "Propiedades" del menú "Acciones".  *Ilustración 72 - Propiedades de los ficheros*

59.	Para evitar, que una vez completado el fichero de registro, se empiece a borrar por la entrada más antigua para reutilizar espacio, y dado que en muchas ocasiones las necesidades de seguridad de una organización priman, debe marcar la opción que permite no perder registros, pero evitando crear grandes ficheros (que podrían afectar al rendimiento): "Archivar el registro cuando esté lleno; no sobrescribir eventos". Pulse sobre "Aceptar" para aplicar esta configuración. Repita este paso sobre el registro "Operativo".  *Ilustración 73 - Archivar el registro cuando esté lleno*
60.	Con la configuración establecida, cuando se alcancen los 1028 kB se archivará el fichero con el nombre: **"Archive-Microsoft IIS-Configuration%4Operational-[año]-[mes]-[día]-[hora]-[minuto]-[segundo]-[milésima de segundo].evtx".** **Nota:** Estos ficheros deberán ser copiados y eliminados periódicamente para evitar su pérdida y el llenado del disco duro.
61.	El servidor se encuentra configurado con todos los parámetros básicos de seguridad.
62.	Ya puede cerrar todas las consolas abiertas y eliminar los archivos utilizados durante el paso a paso.
63.	Finalmente, inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en un Controlador de Dominio.

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

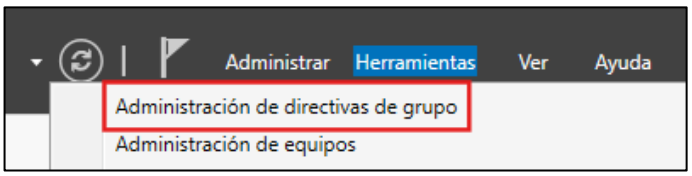


Ilustración 74 - Administración de directivas de grupo

65.	Despliegue el panel izquierdo hasta llegar a la OU “Domain Controllers”.

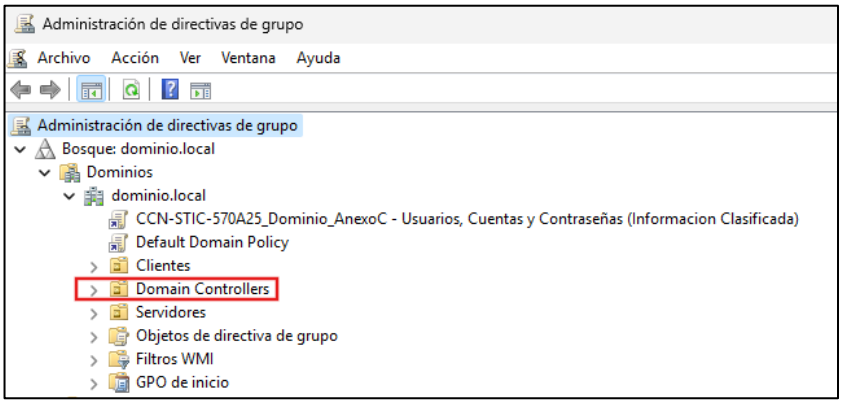


Ilustración 75 - OU Domain Controllers

66.	Despliegue dicha OU, haga clic derecho sobre el GPO “CCN-STIC-570A25_DC_AnexoA – ADMX (Nivel de Clasificación)”, y seleccione “Editar”.

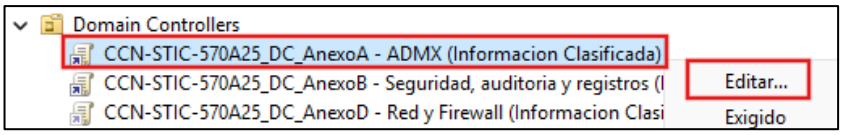
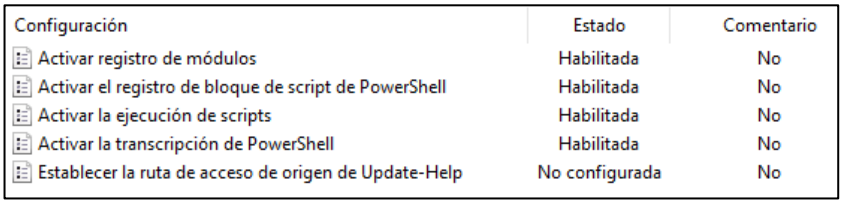


Ilustración 76 - Edición ADMX 570A25

67.	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



Configuración	Estado	Comentario
Activar registro de módulos	Habilitada	No
Activar el registro de bloque de script de PowerShell	Habilitada	No
Activar la ejecución de scripts	Habilitada	No
Activar la transcripción de PowerShell	Habilitada	No
Establecer la ruta de acceso de origen de Update-Help	No configurada	No

Ilustración 77 - Políticas de PowerShell

68.	Haga doble clic sobre la política “Activar la ejecución de scripts”.

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

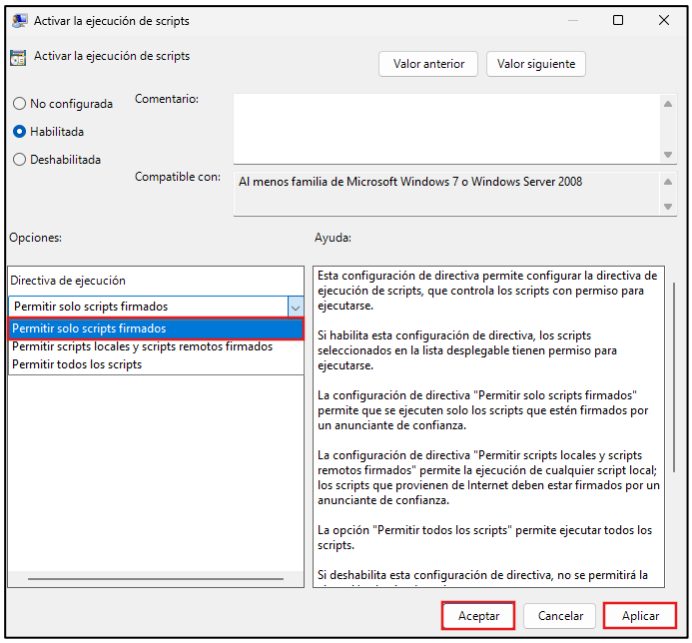
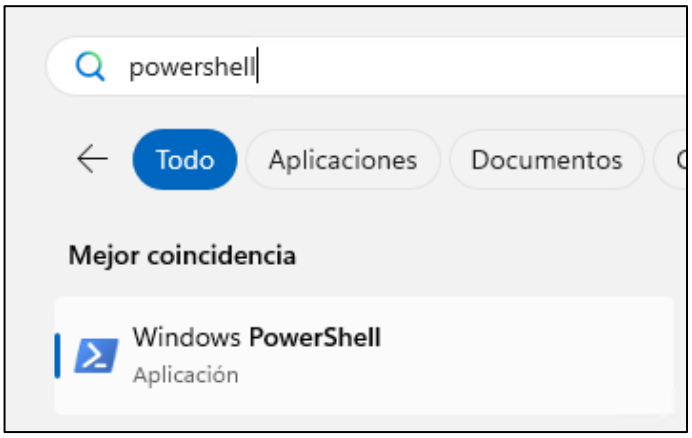
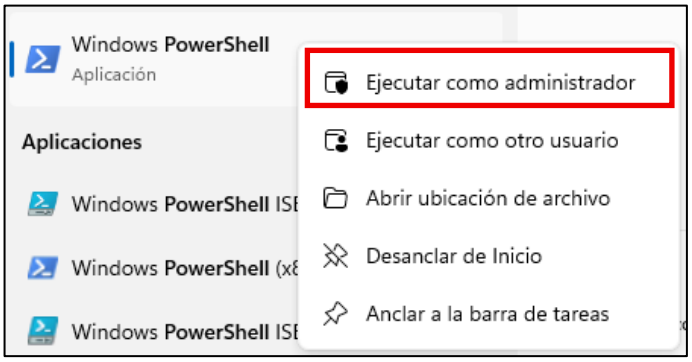
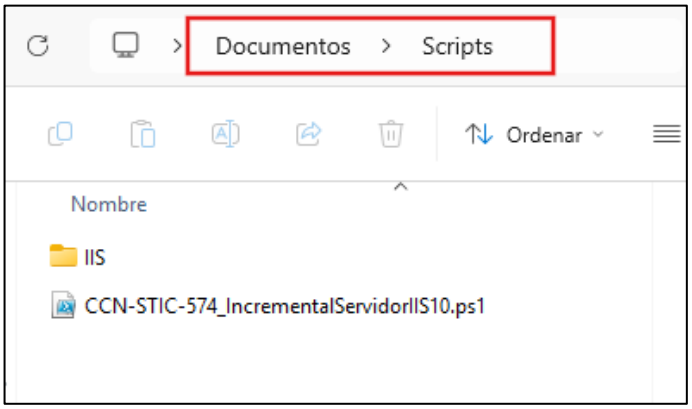


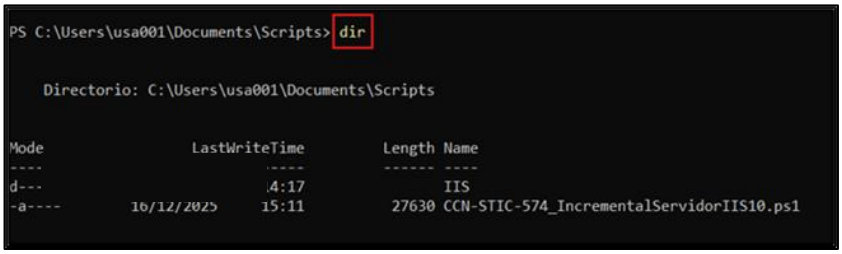
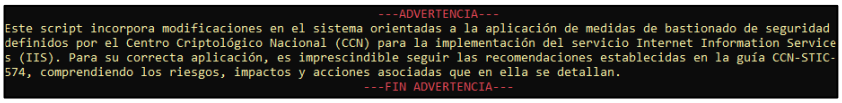
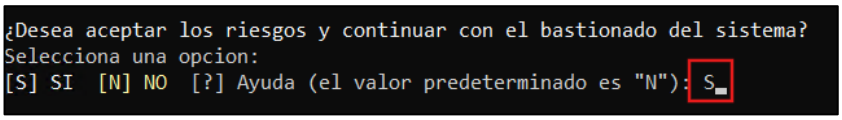
Ilustración 78 - Selección de "Permitir solo scripts firmados"

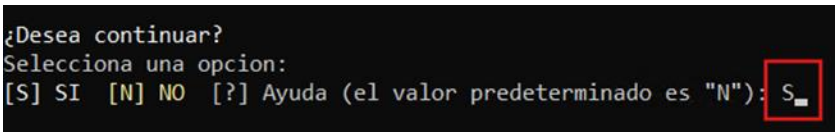
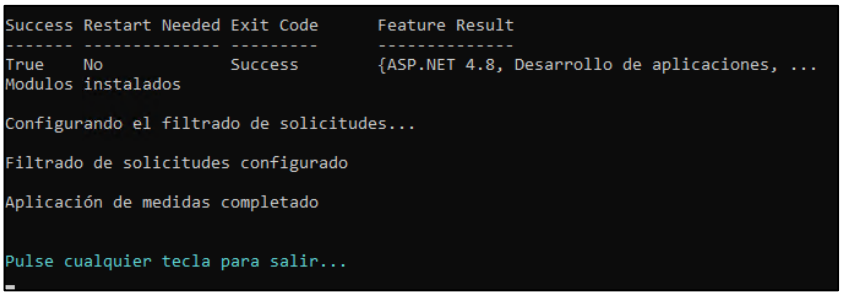
ANEXO A.1.3. PASO A PASO DE CONFIGURACIÓN DE SEGURIDAD EN SERVIDOR WEB DINÁMICO

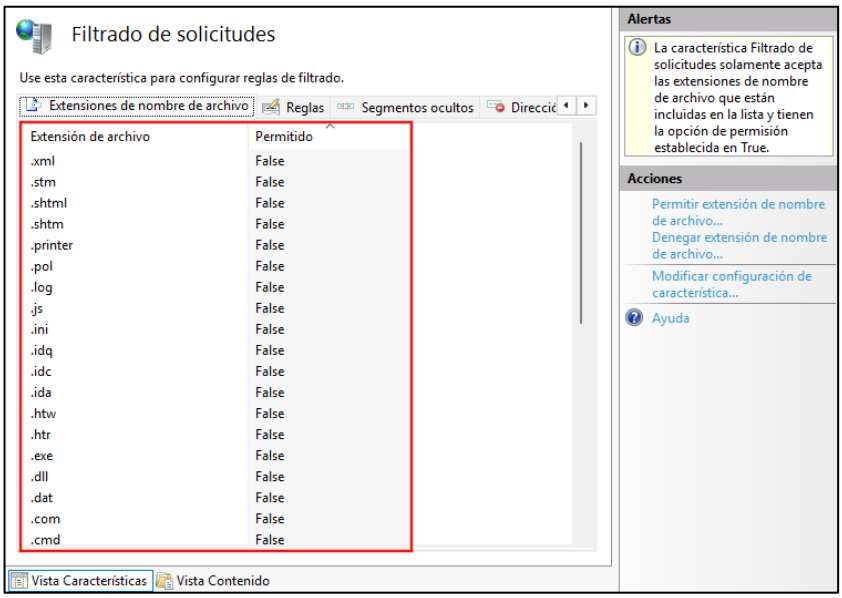
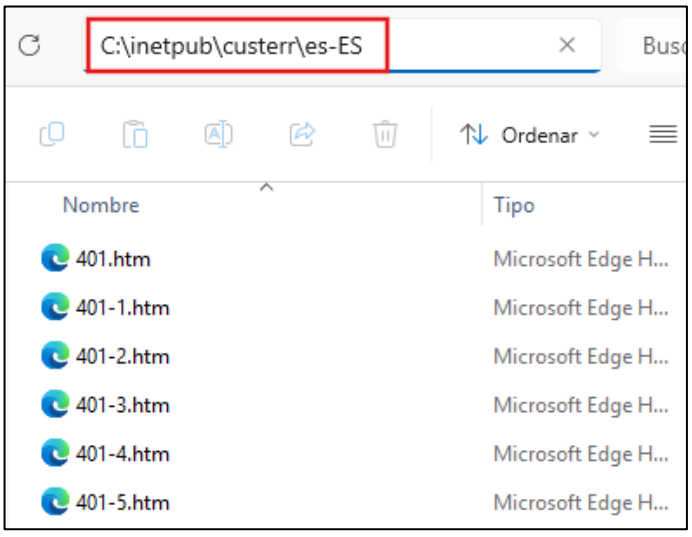
Paso	Descripción
1.	Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en el Servidor IIS.
2.	Copie los ficheros y directorios que acompañan a esta guía al directorio en la carpeta “**Documentos**” del usuario administrador. A continuación, descomprima la carpeta. Verifique que en su interior se encuentran los siguientes archivos: - Directorio: IIS - Fichero: CCN-STIC-574_IncrementalServidorIIS10.ps1

Ilustración 79 - Copia de ficheros necesarios

3.	Sobre la barra de búsqueda, escriba “PowerShell”:  *Ilustración 80 - Windows PowerShell*
4.	Haga clic derecho, y seleccione “Ejecutar como administrador”:  *Ilustración 81 - 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.
5.	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 82 - Copia de ruta*

6.	Desde la ventana de PowerShell, utilizando el comando “cd”, acceda a la ruta recientemente copiada.  *Ilustración 83 - Acceso a la ruta*
7.	Ejecute el comando “dir” para verificar la ubicación y el contenido.  *Ilustración 84 - Contenido de la carpeta*
8.	Ejecute el archivo “CCN-STIC-574_IncrementalServicioIIS10.ps1” escribiendo “.\” y pulsando la tecla tabuladora hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución.  *Ilustración 85 - Ejecución del script*
9.	A continuación, se mostrará una advertencia de uso, continuando con el siguiente mensaje:  *Ilustración 86 - Advertencia*
10.	Escribir “S” y pulsar “Enter”.  *Ilustración 87 - Aceptación de advertencia*

11.	Aparecerán dos opciones de configuración: - [A] Web Estática - [B] Web Dinámica Escribir “B” y continuar con la configuración del servidor.  *Ilustración 88 - Opciones instalación*
12.	Espere a que termine la ejecución. Una vez hecho, deberá escribir “S” y pulsar “Enter” para continuar con la configuración.  *Ilustración 89 - Continuar*
13.	Una vez haya terminado, pulsar cualquier tecla para salir.  *Ilustración 90 - Finalización del script*

14.	Se habrá incorporado el "filtrado de solicitudes" del entorno de administración. Acceda y revise todas las pestañas para comprobar que "Extensiones de nombre de archivo" incorpora un listado con todos los valores no permitidos, figuran como "False", y "Segmentos ocultos" tiene varias entradas, entre ellas web.config. **"Menú inicio > Herramientas administrativas > Administrador de Internet Information Services (IIS) > [nombre_del_servidor] > Filtrado de solicitudes".**  *Ilustración 91 - Filtrado de solicitudes*
15.	Verifique que la carpeta **"C:\Inetpub\custerr\es-ES\"** existe, ya que se utilizará para evitar mostrar información adicional a posibles atacantes mediante mensajes de error detallados.  *Ilustración 92 - Carpeta de mensajes de error* **Nota**: la ruta será diferente si se ha especificado otro volumen en el entorno.

16. En dicha carpeta debe alojar el archivo **"error.htm"**, incluido en el directorio **"IIS"** dentro de la carpeta de la guía. Este archivo será el mensaje de error estándar que se mostrará independientemente de la causa que lo genere.

Ilustración 93 - Archivo error.htm

17. Los permisos locales (permisos NTFS) de la carpeta **"C:\Inetpub\custerr"** estarán asignados como los que se muestran en la siguiente tabla, de no ser así, en su servidor, deberá hacer los cambios necesarios.

Carpeta	Grupo/Usuario	Permiso NTFS
C:\Inetpub\custerr	CREATOR OWNER	Permiso especial: Control total solo esta subcarpeta y archivos
	SYSTEM	Control total
	Administradores	Control total
	Usuarios	Lectura y Ejecución
	TrustedInstaller	Control total

18. Sobre la barra de búsqueda, escriba "Administrador de Internet Information Services (IIS)".

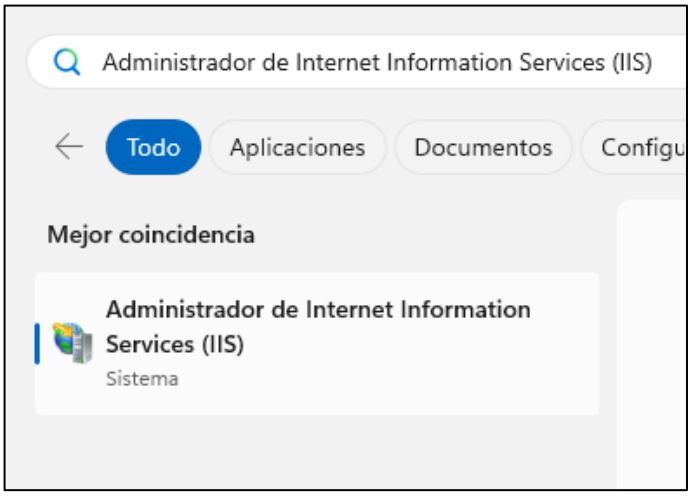


Ilustración 94 - Administrador de Internet Information Sevices

19.	Haga clic derecho y seleccione “Ejecutar como administrador”.
20.	En el árbol de conexiones, sitúese sobre el nodo “Administrador de Internet Information Services (IIS) > [nombre_del_servidor]”.

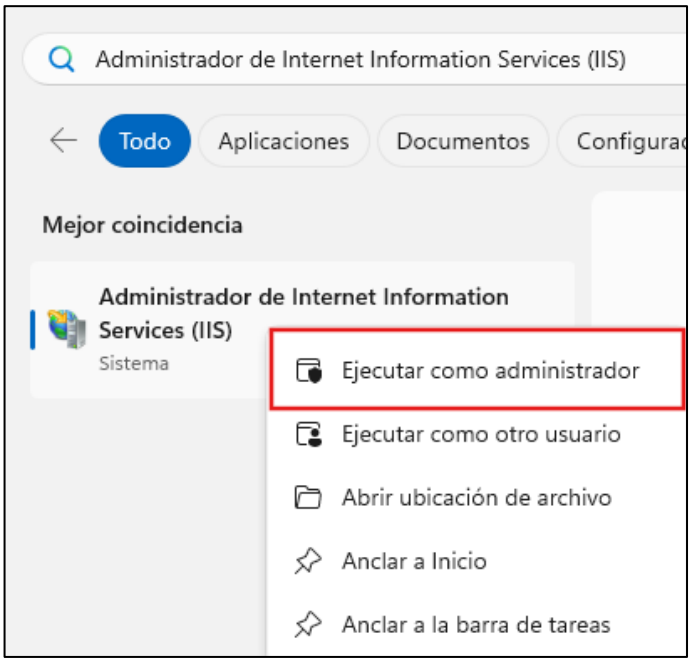


Ilustración 95 - Ejecutar como administrador

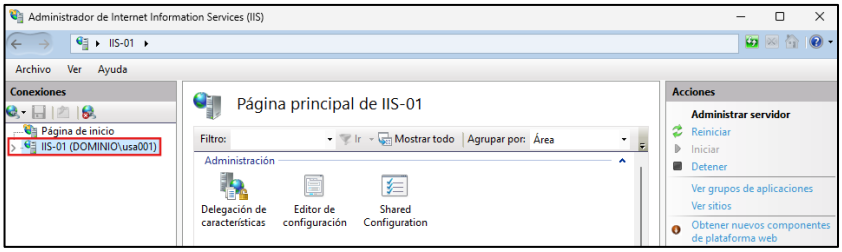
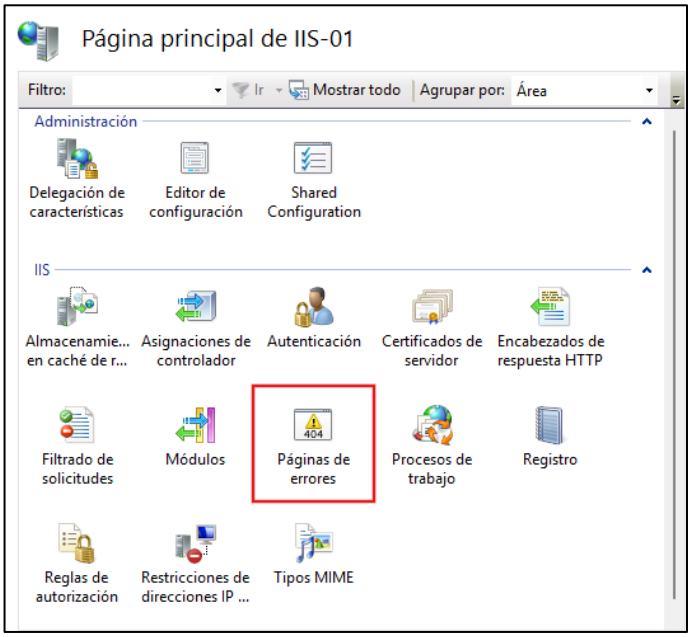
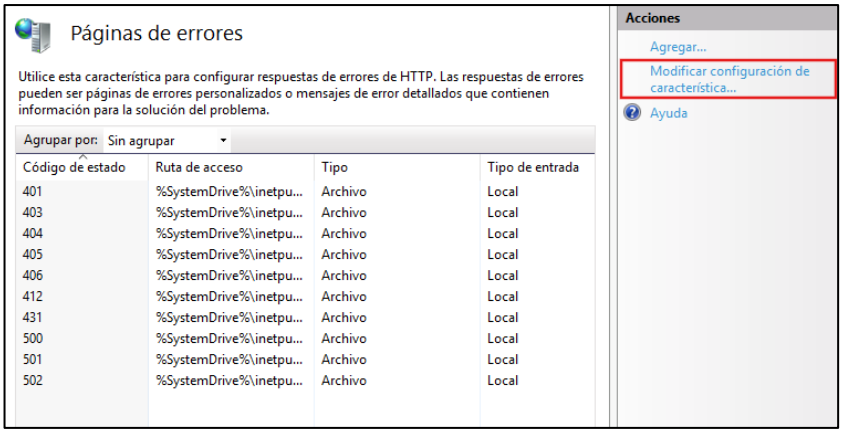
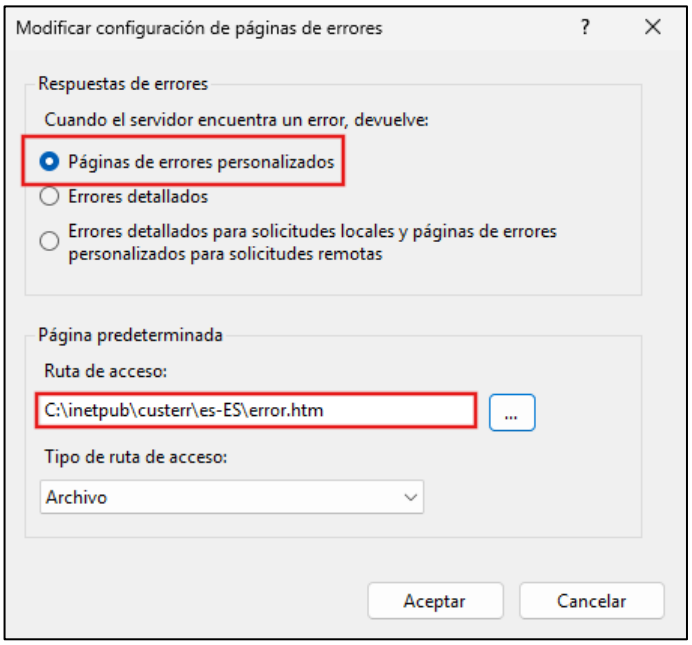
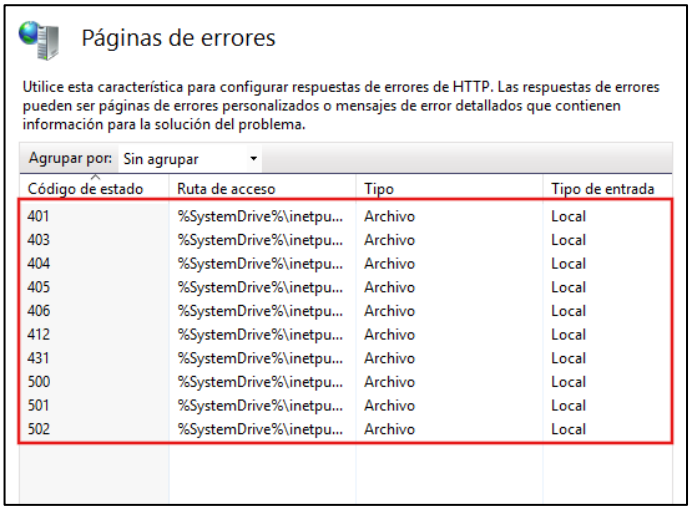
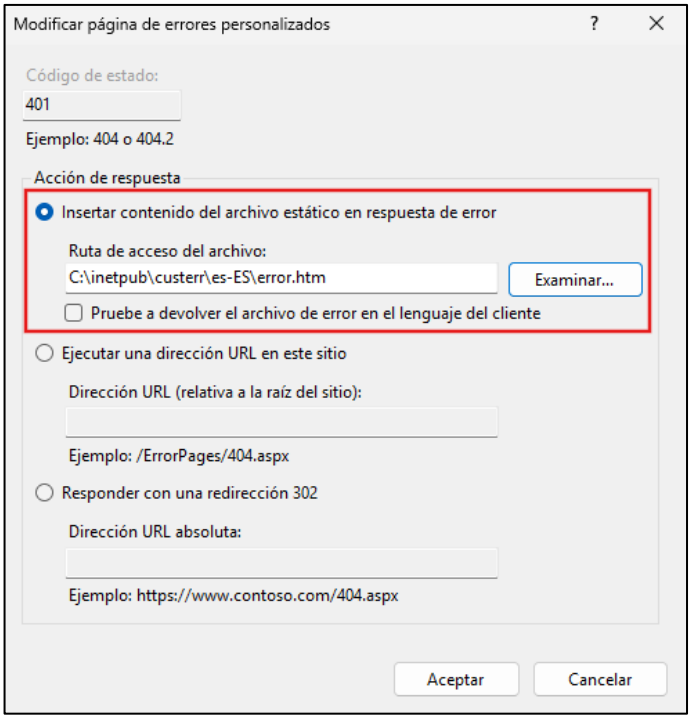
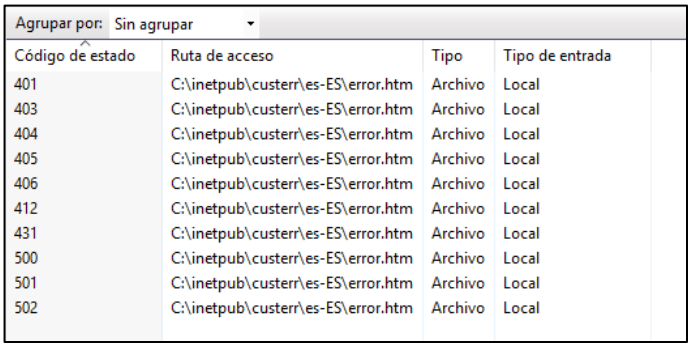
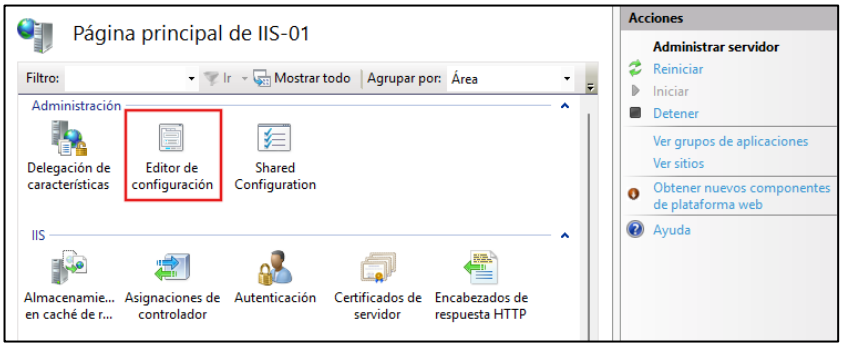
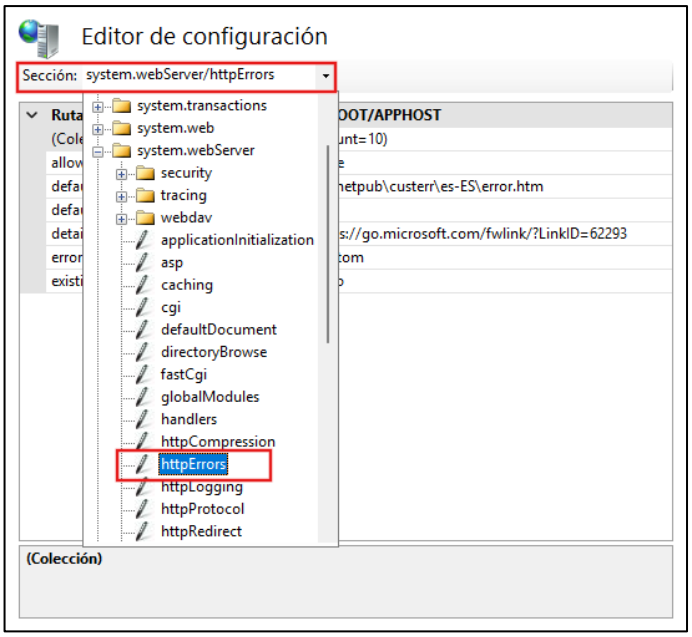


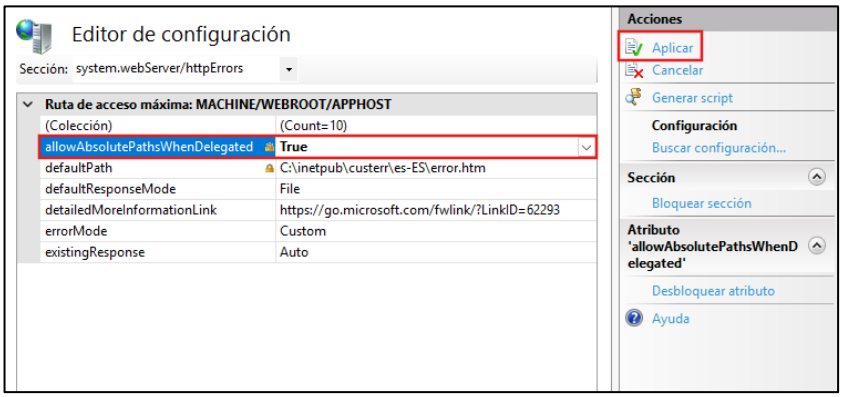
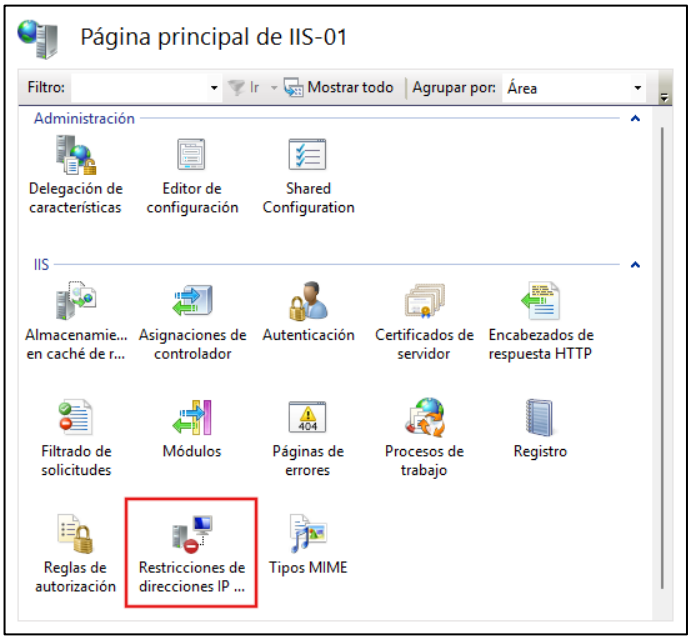
Ilustración 96 - Página principal de IIS

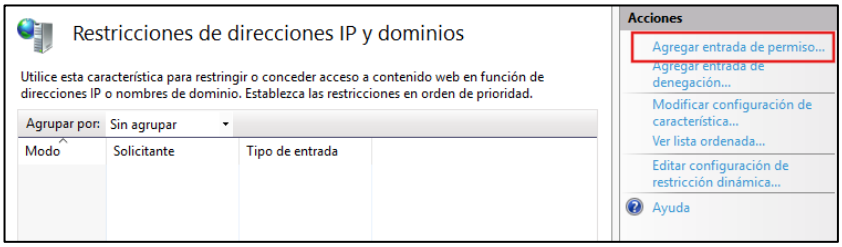
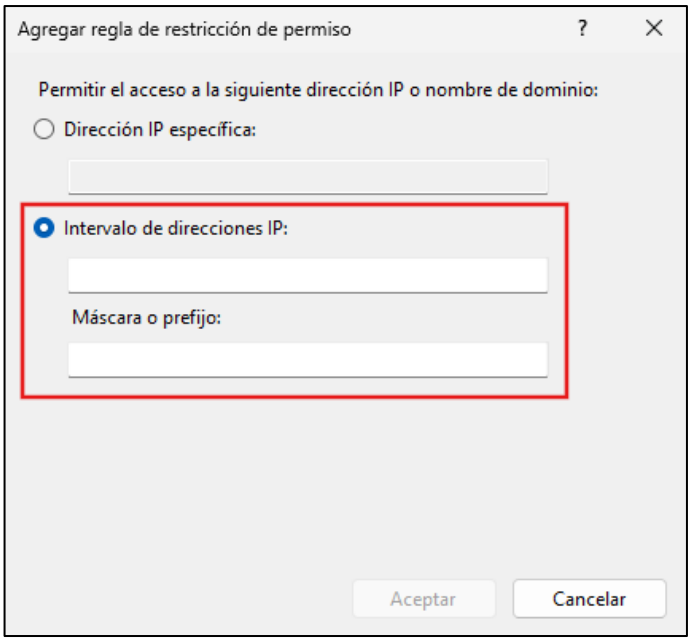
21.	Seleccione “Páginas de errores” en el menú central.  *Ilustración 97 - Página de errores*
22.	Una vez abierta la característica, seleccione en el menú “Acciones”, en el lateral derecho, “Modificar configuración de característica…”.  *Ilustración 98 - Modificar página de errores*

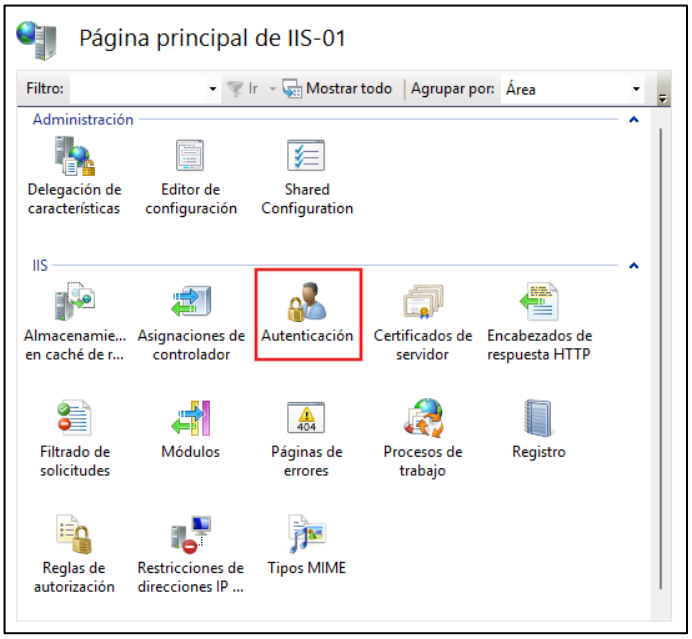
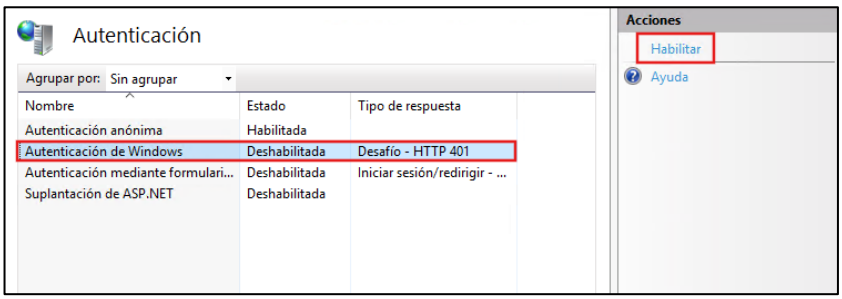
23.	Ahora elija el fichero copiado en pasos anteriores, "**error.htm**", como error personalizado por defecto. Pulse "Aceptar" para completar la configuración.  *Ilustración 99 - Configuración de página de errores*
24.	Para la personalización de los errores, y evitar que muestren información que podría ayudar a posibles atacantes a crear un perfil de sus sistemas, termine la personalización de todos los errores que se muestran en la lista de página de errores.  *Ilustración 100 - Códigos de errores*

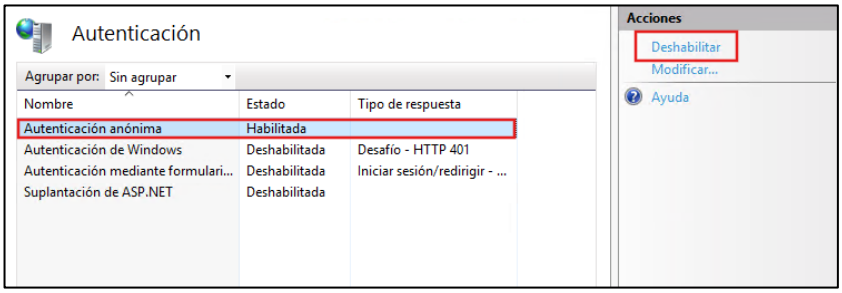
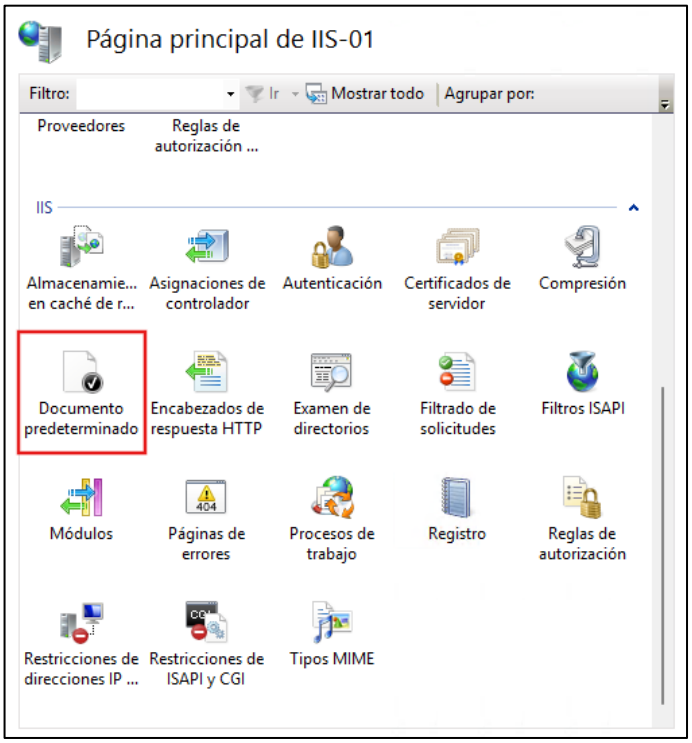
25.	Para cada código de estado, seleccione la línea y haga clic en “Modificar…” en el menú “Acciones”. Configure los errores con los valores indicados a continuación. - Seleccione “Insertar contenido del archivo estático en respuesta de error”. - Desmarque “Pruebe a devolver el archivo de error en el lenguaje del cliente”. - Ruta de acceso del archivo: C:\inetpub\custerr\es-ES\error.htm Pulse sobre “Aceptar” para finalizar la configuración.  *Ilustración 101 - Modificación de códigos de errores*
26.	Cuando termine se mostrará la ventana de errores siguiente.  *Ilustración 102 - Ventana de errores configurada*

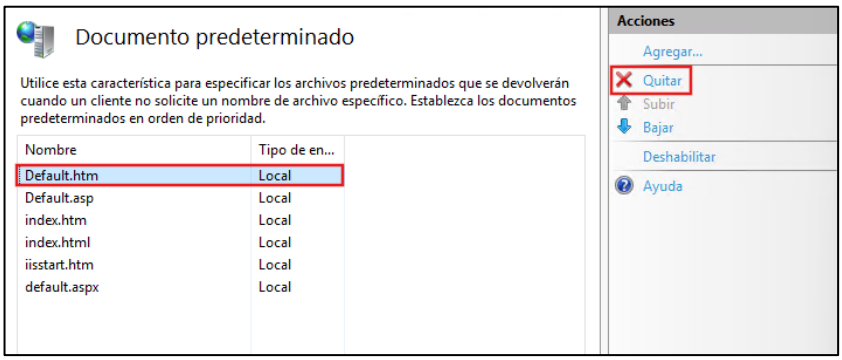
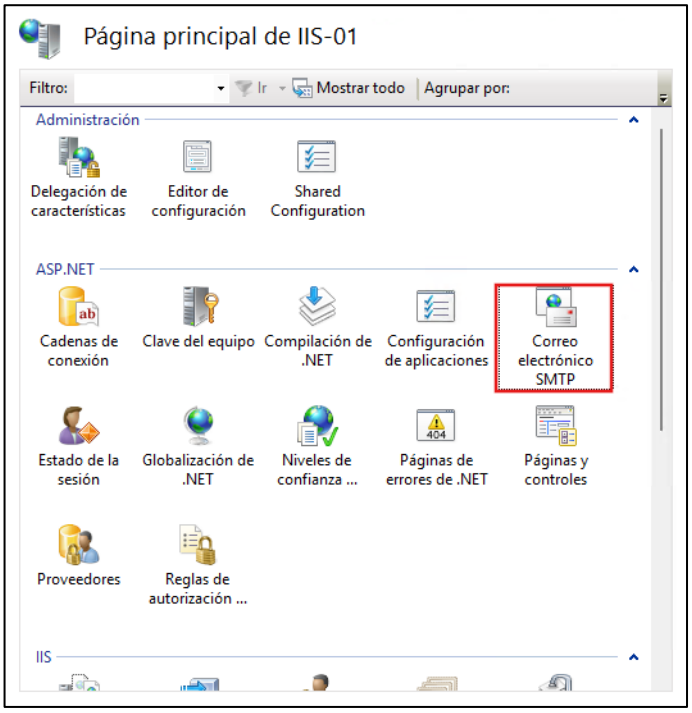
27.	Edite el archivo applicationHost.config para habilitar el uso de rutas absolutas. Vuelva a situarse sobre el servidor y seleccione **"Editor de configuración". "Menú inicio > Herramientas administrativas > Administrador de Internet Information Services (IIS) > [nombre_del_servidor] > Editor de configuración".**  *Ilustración 103 - Editor de configuración*
28.	En la lista desplegable "Sección" marque "system.webServer/httpErrors".  *Ilustración 104 - httpErrors*

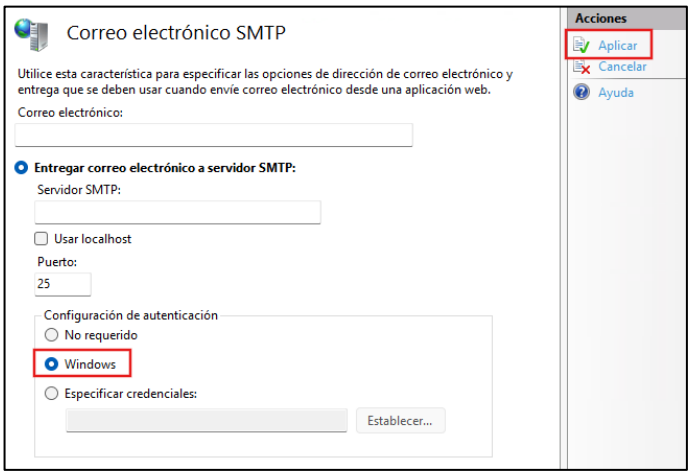
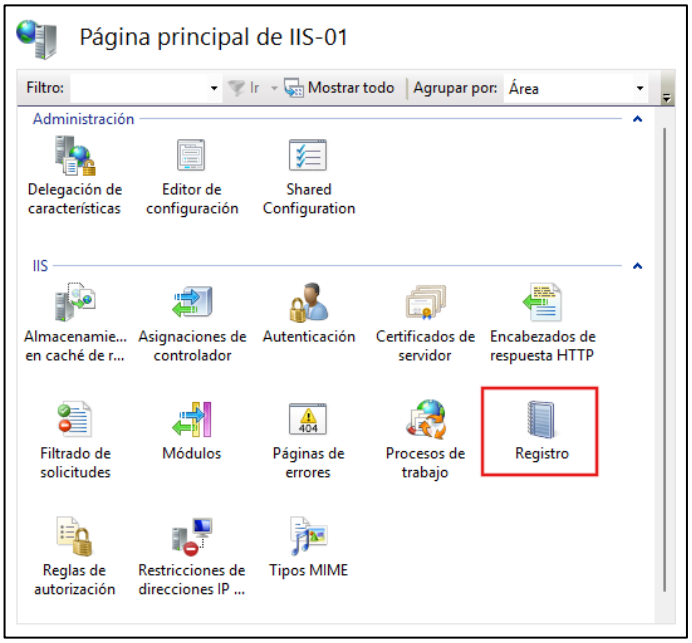
29.	Cuando se abra la ventana cambie la variable “allowAbsolutePathsWhenDelegated” a “True” y seleccione “Aplicar” en el menú” Acciones”.  *Ilustración 105 - allowAbsolutePathsWhenDelegated en "True"*
30.	Ahora va a limitar el acceso al servidor según las direcciones IP de su red. Vuelva a la página principal del servidor IIS.
31.	Acceda a la funcionalidad “Restricciones de direcciones IP y dominios”. **“Administrador de Internet Information Services (IIS) > [nombre_del_servidor] > Restricciones de direcciones IP y dominios”**  *Ilustración 106 - Restricciones de direcciones IP*

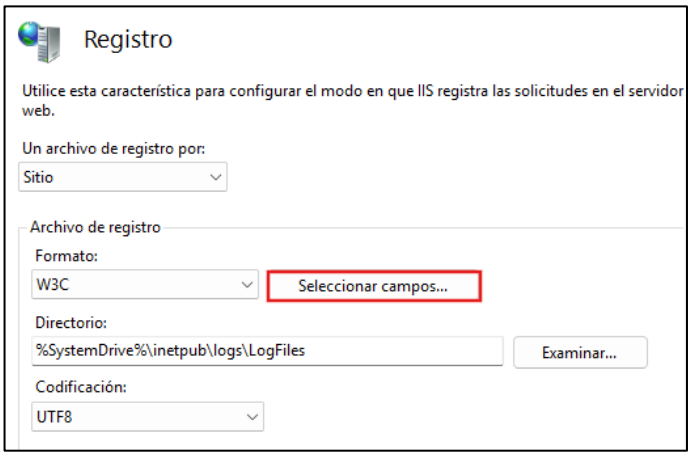
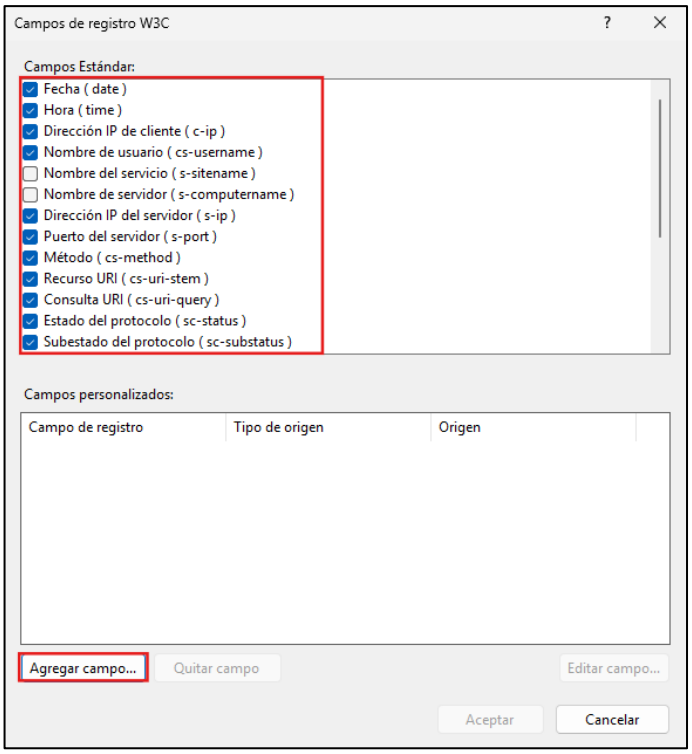
32.	Se abrirá una ventana sin ninguna regla creada, por lo que debe incluir las redes que tendrán acceso al servidor. Para ello, seleccione la opción "Agregar entrada de permiso…" en el panel "Acciones".  *Ilustración 107 - Agregar entrada de permiso*
33.	Introduzca el rango de direcciones IP correspondiente a su red LAN. El ejemplo asume que el servidor está dentro de ese rango.  *Ilustración 108 - Intervalo de direcciones IP* **Nota:** La red que se ha incluido es la propia del ejemplo, es indispensable que adapte este paso a su entorno. Si no conoce la red o subred donde se alojan los equipos consulte con su administrador de redes. Su entorno podría incluir más de una subred, puede agregar cuantas reglas como sean necesarias.

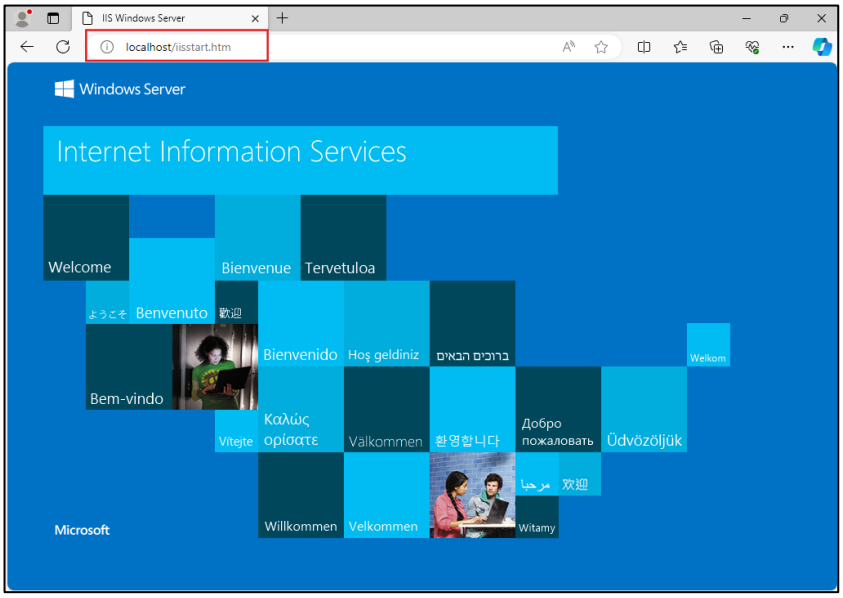
34.	Ahora va a configurar la autenticación a utilizar en su entorno. Acceda a la herramienta de administración de IIS, sección "Autenticación". **"Menú inicio > Herramientas administrativas > Administrador de Internet Information Services (IIS) > [nombre_del_servidor] > Autenticación"**  *Ilustración 109 - Autenticación*
35.	Proceda a habilitar el método "Autenticación de Windows" para que esté operativo. Seleccione "Autenticación de Windows" y en el panel "Acciones" pulse sobre "Habilitar".  *Ilustración 110 - Habilitar autenticación de Windows*

36.	Intentando minimizar el riesgo, si todos sus clientes están autenticados por el dominio y acceden a este servidor por la red LAN, debería deshabilitar la autenticación anónima. Para ello seleccione “Autenticación anónima” y “Deshabilitar”.  *Ilustración 111 - Deshabilitar autenticación anónima*
37.	Acceda a la herramienta de administración de IIS, a la sección de “Documento predeterminado”. **“Menú inicio > Herramientas administrativas > Administrador de Internet Information Services (IIS) > [nombre_del_servidor] > Documento predeterminado”.**  *Ilustración 112 - Documento predeterminado*

38.	Dentro de este servicio del rol IIS, Documento predeterminado, solo deberían figurar aquellos archivos que sean indispensables para el funcionamiento de sus respectivos sitios web, por eso se recomienda eliminar todas las entradas del servidor y agregar a cada sitio aquellos que sean necesarios. Seleccione cada uno de los documentos predeterminados y haga clic en "Quitar", confirme la eliminación seleccionando "Sí", también para cada uno de los documentos.  *Ilustración 113 - Deshabilitar documentos predeterminados*
39.	Cuando instaló los módulos relacionados con ASP.NET se incluyó el servidor SMTP de correo electrónico. Acceda a configurarlo. **"Menú inicio > Herramientas administrativas > Administrador de Internet Information Services (IIS) > [nombre_del_servidor] > Correo electrónico SMTP".**  *Ilustración 114 - Correo electrónico SMTP*

40.	Por defecto, queda con una configuración de autenticación que podría ser vulnerable, ya que si no hay autenticación puede utilizarse el servidor para el envío de correo fraudulento usándolo como open relay, o relay abierto. Para evitarlo seleccione la opción “Windows” en el apartado “Configuración de autenticación”. Pulse “Aplicar” en la columna “Acciones” para confirmar los cambios.  *Ilustración 115 - Configuración de autenticación Windows*
41.	Acceda a la herramienta de administración de IIS, sección “Registro”. **“Menú inicio > Herramientas administrativas > Administrador de Internet Information Services (IIS) > [nombre_del_servidor] > Registro”.**  *Ilustración 116 - Registro*

42.	El registro queda habilitado con los valores por defecto después de la instalación. Haga clic en “Seleccionar campos…” para personalizar el registro.  *Ilustración 117 - Campos de registro*
43.	Compruebe qué campos se recogerán en el fichero de registro y asegúrese que coincide con las necesidades del entorno. Los valores marcados por defecto suelen ser suficientes, pero no descarte marcar otros.  *Ilustración 118 - Comprobación de campos* **Nota:** Existe la posibilidad de incluir en esta ventana campos personalizados.

44.	Para conseguir que se cree la carpeta donde se van a alojar las subcarpetas de registro de cada sitio web, "**C:\inetpub\logs\logfiles**", es necesario generar, al menos un acceso. Para ello, abra Microsoft Edge desde el Menú inicio del servidor IIS y acceda a la URL http://localhost/iisstart.htm  *Ilustración 119 - URL inicial*
45.	En los pasos siguientes se le detalla cómo configurar los permisos locales, permisos NTFS, de la carpeta "**C:\inetpub\logs\logfiles**", que deben quedar como los que se muestran en la siguiente tabla.

Carpeta	Grupo/Usuario	Permiso NTFS
C:\inetpub\logs\logfiles	CREATOR OWNER	Permiso especial: Control total solo esta subcarpeta y archivos
	SYSTEM	Control total
	Administradores	Control total
	Auditores	Leer
	TrustedInstaller	Control total

46.	Abra el Explorador de archivos y diríjase a la carpeta "**C:\inetpub\"**, con el botón derecho, sobre la carpeta **logs**, selecciones "Propiedades".

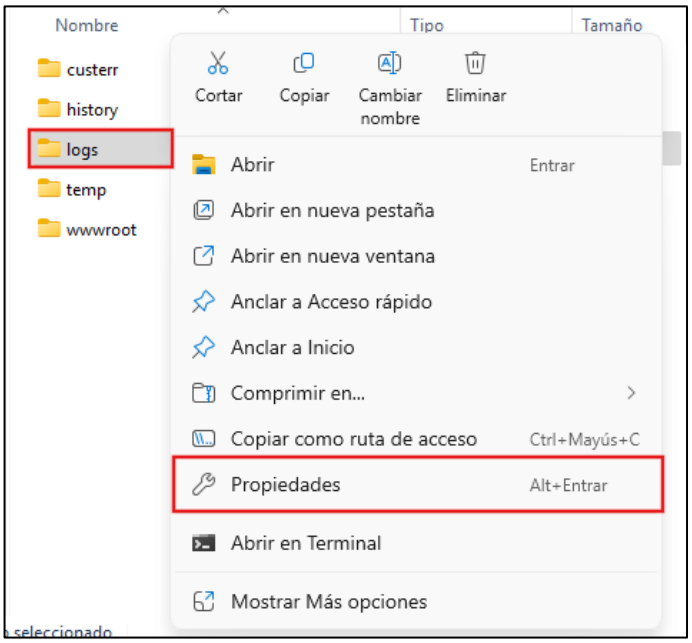


Ilustración 120 - Propiedades de logs

47.	Sitúese en la pestaña “Seguridad”, donde observa que la carpeta tiene permisos aplicados directamente. Presiones “Editar” para modificar los permisos.

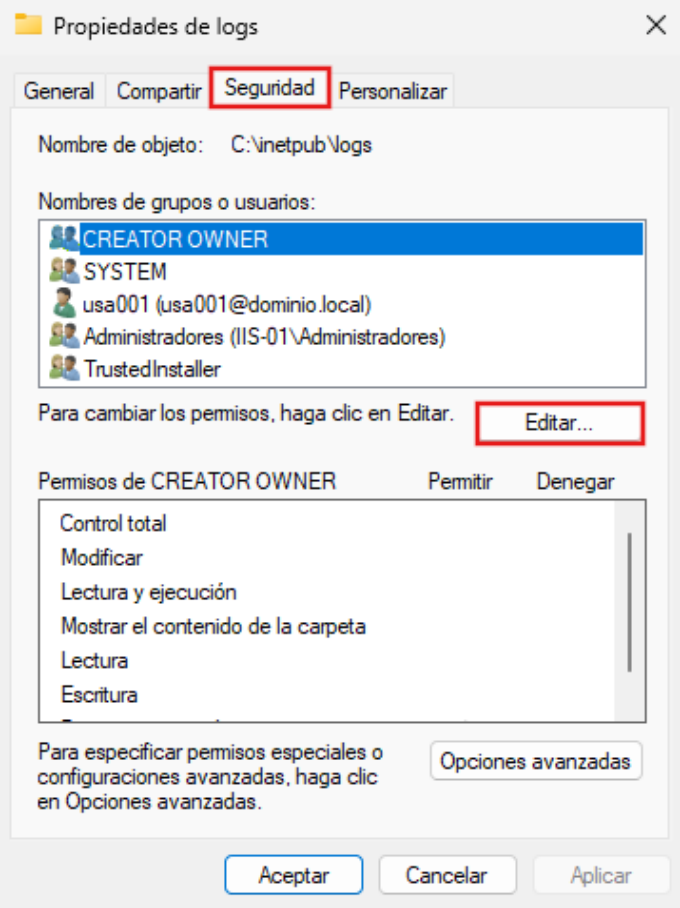
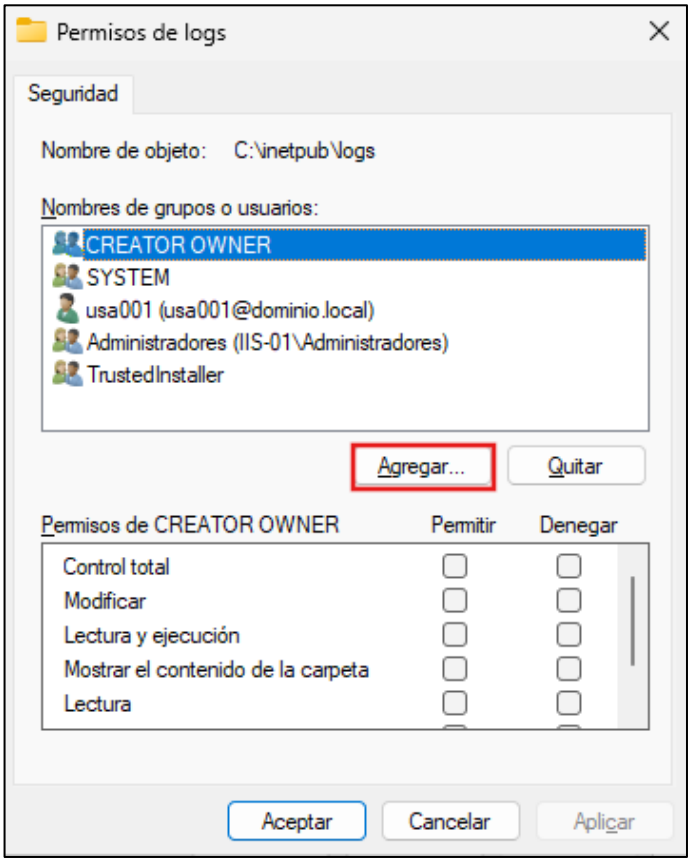
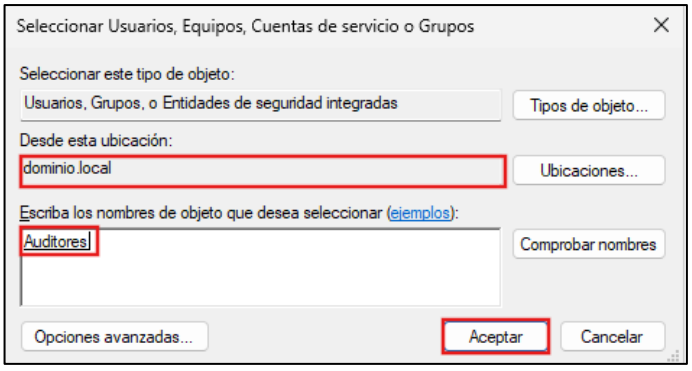
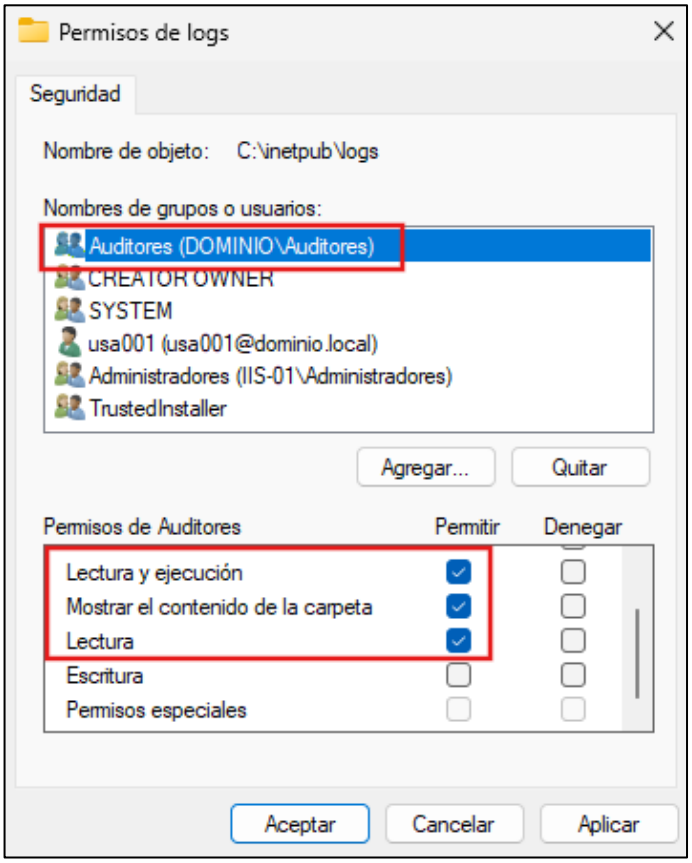
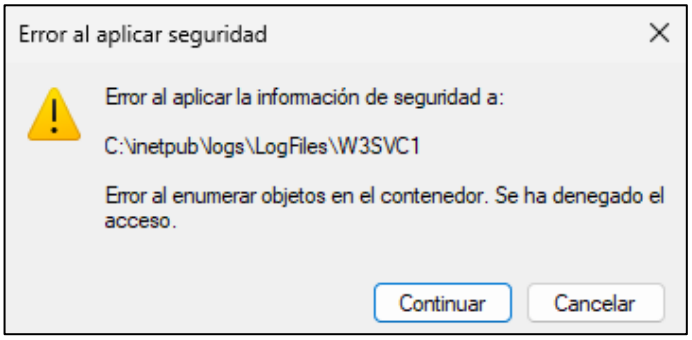
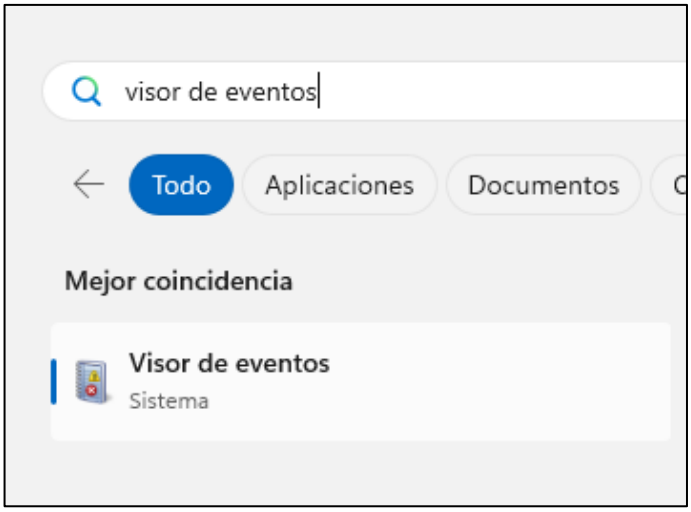
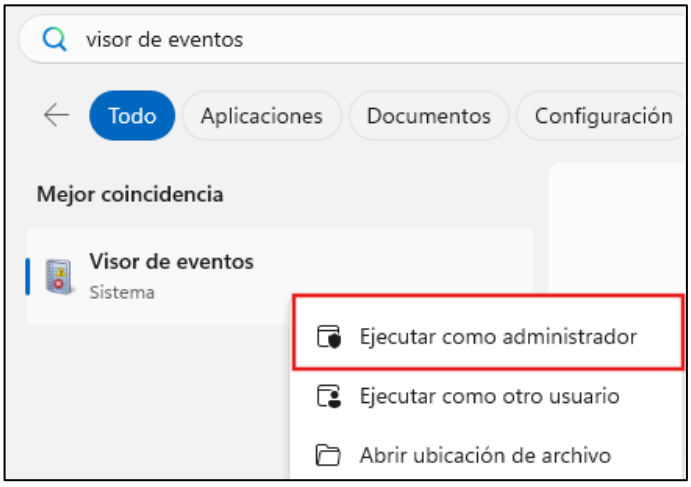


Ilustración 121 - Pestaña de seguridad

48.	Presione el botón “Agregar…”, para en los siguientes pasos añadir el grupo “Auditores”.  *Ilustración 122 - Agregar permisos*
49.	Escriba “Auditores” y acepte para que se añada.  *Ilustración 123 - Agregar grupo de Auditores* **Nota:** Existe la posibilidad de que el grupo “Auditores” no exista de forma predeterminada en el dominio. En ese caso, cree el grupo en un servidor Controlador de Dominio o seleccione un grupo que sea el encargado de llevar a cabo la tarea de Auditores.

50.	Los permisos que se adjudican por defecto, para los “Auditores” son los siguientes.  *Ilustración 124 - Permisos de auditores*
51.	En algunas circunstancias, se le puede mostrar un mensaje como el siguiente, ya que los permisos de la carpeta **“C:\inetpub\logs\”** están marcados para ser actualizados por herencia, recibirán los nuevos permisos automáticamente. Presione “Continuar” para conseguir aplicar los cambios  *Ilustración 125 - Mensaje de aviso* **Nota:** El aviso le indica que los cambios no se aplicarán sobre la carpeta” W3SVC1” y los ficheros que contenga. La carpeta es la propia del registro del Default Web Site. Para cada sitio web alojado en el servidor se creará una carpeta específica que se alojará en el mismo camino que la del Defaul Web Site.

52.	En los siguientes pasos va a activar la auditoría del servidor. En este caso se permitirá registrar acciones sobre los servicios y no de acceso de usuarios, como en el “Registro”, configurado en pasos anteriores.
53.	Sobre la barra de búsqueda, escriba “Visor de eventos”.  *Ilustración 126 - Visor de eventos*
54.	Haga clic derecho y seleccione “Ejecutar como administrador”.  *Ilustración 127 - Ejecutar modo administrador*

55.	Despliegue el siguiente nodo. **"Visor de eventos (local) > Registro de aplicaciones y servicios > Microsoft > Windows > IIS-Configuration".**

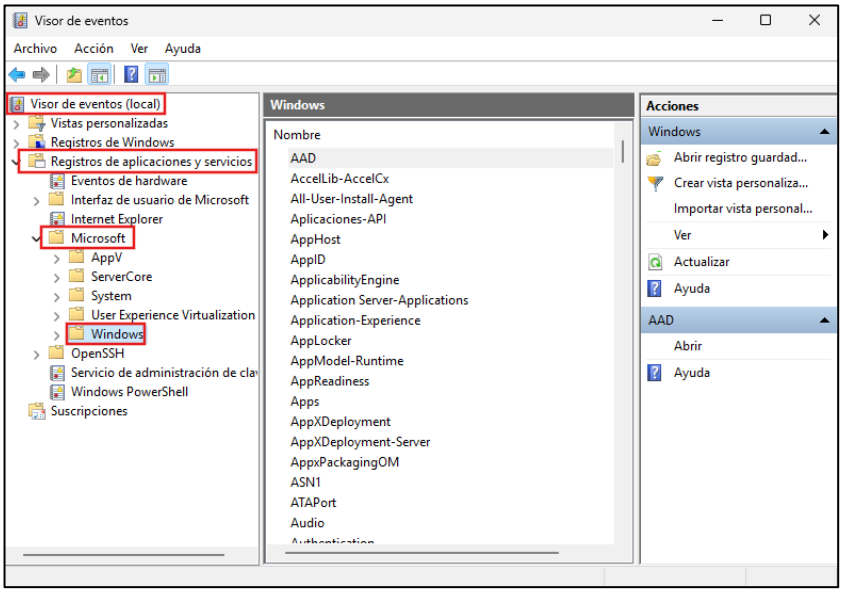


Ilustración 128 - Carpeta del visor de eventos

56.	Windows Server 2025 dispone de dos grupos de registros para IIS, dentro del nodo de configuración se encuentran el registro administrativo y el registro operativo. Es necesario activar ambos.

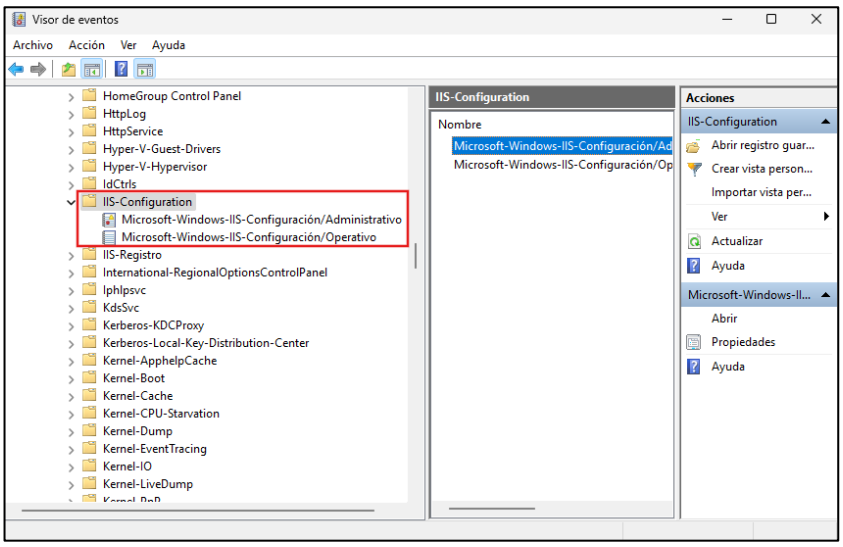


Ilustración 129 - Registros

57.	Sitúese sobre el registro “Administrativo”, abra el menú contextual con el botón derecho del ratón y seleccione “Habilitar registro”.

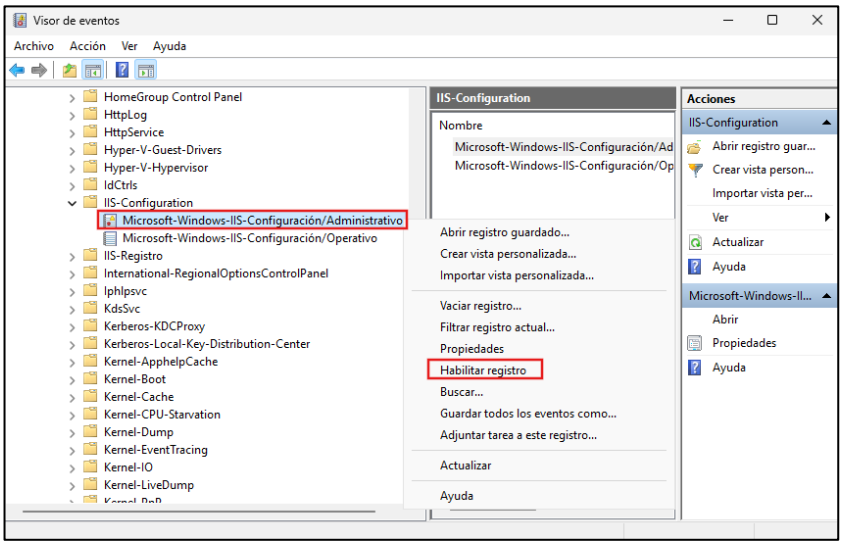


Ilustración 130 - Habilitar registro administrativo

58.	Haga lo mismo para el registro “Operativo.”

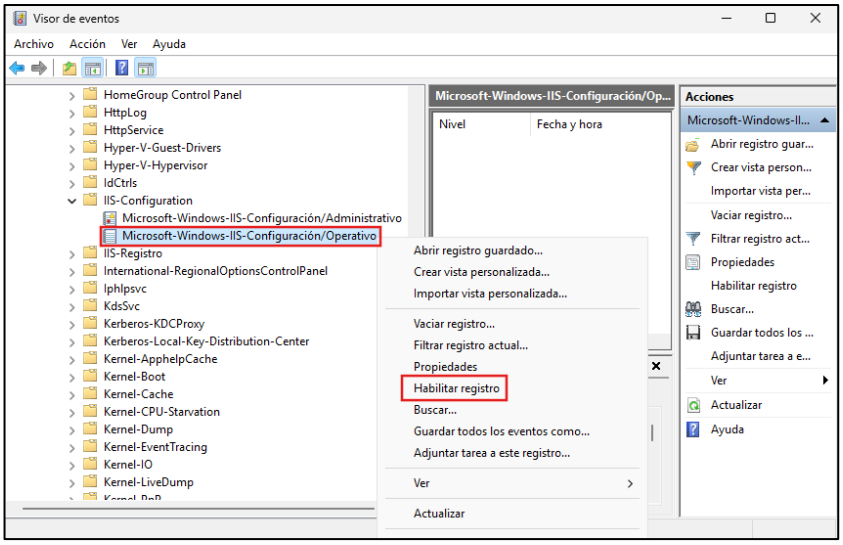
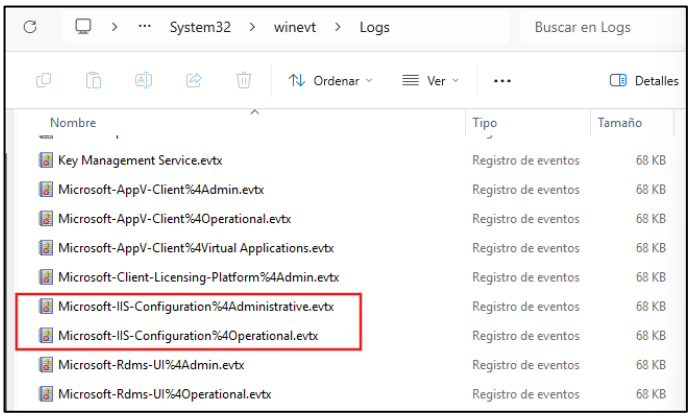
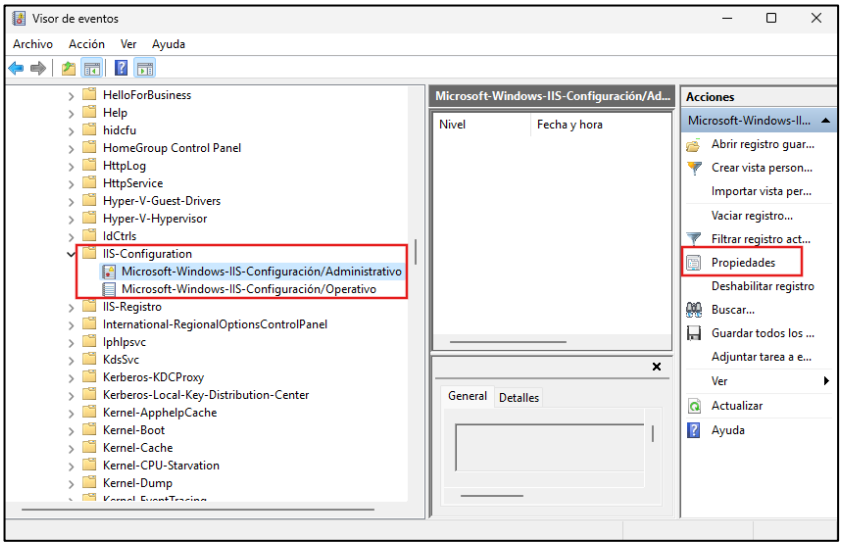
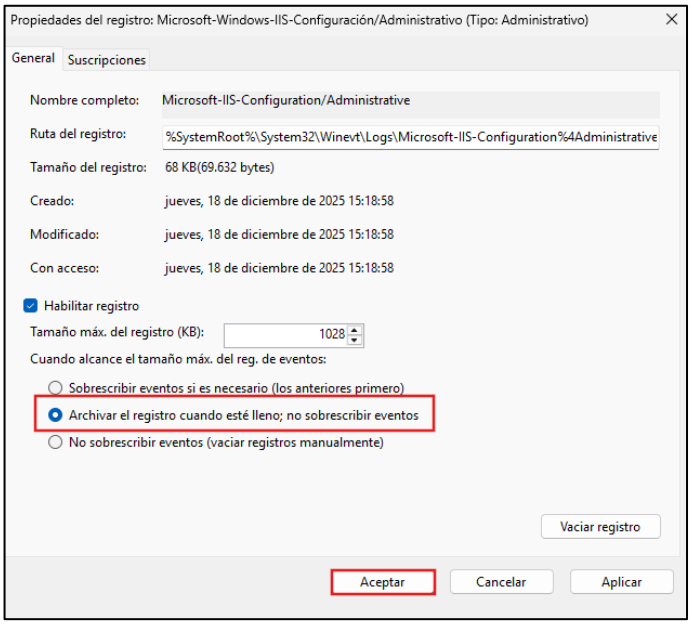
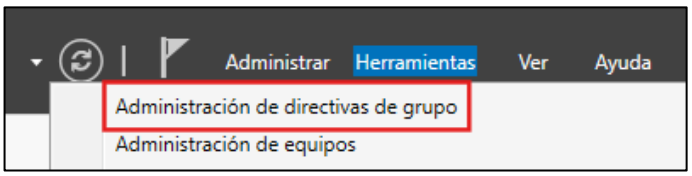
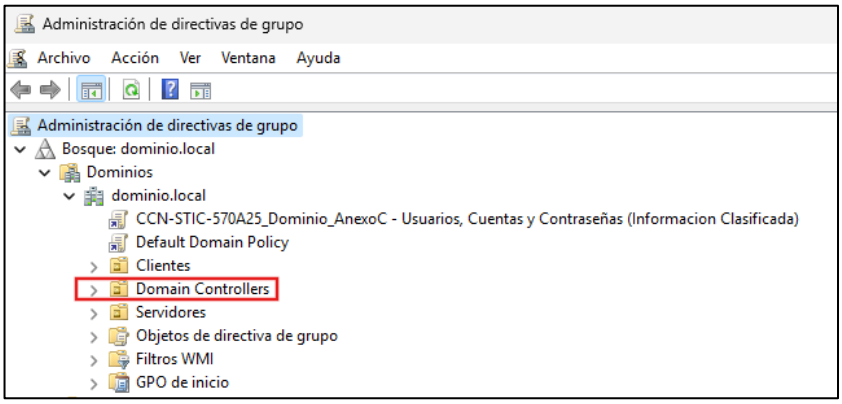
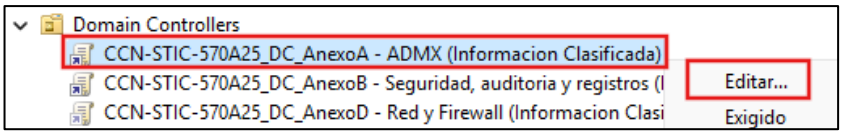
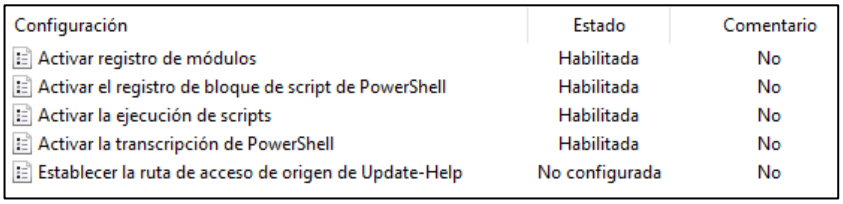


Ilustración 131 - Habilitar registro operativo

Cualquier acción operativa y administrativa realizada sobre el servidor quedará recogida a partir de ahora.

59.	Los registros se habrán creado en el disco duro, en la partición del sistema operativo (habitualmente en "C:\") en la ruta **"%SystemRoot%\System32\winevt\Logs"**, con los nombres: Microsoft IIS-Configuration%4Operational.evtx y Microsoft IIS-Configuration%4Administrative.evtx.  *Ilustración 132 - Registros creados*
60.	Para acceder a las propiedades de los ficheros, seleccione un fichero y pulse sobre la opción "Propiedades" del menú "Acciones".  *Ilustración 133 - Propiedades de los ficheros*

61.	Para evitar, que una vez completado el fichero de registro, se empiece a borrar por la entrada más antigua para reutilizar espacio, y dado que en muchas ocasiones las necesidades de seguridad de una organización priman, debe marcar la opción que permite no perder registros, pero evitando crear grandes ficheros (que podrían afectar al rendimiento): "Archivar el registro cuando esté lleno; no sobrescribir eventos". Pulse sobre "Aceptar" para aplicar esta configuración. Repita este paso sobre el registro "Operativo".  *Ilustración 134 - Archivar el registro cuando esté lleno*
62.	Con la configuración establecida, cuando se alcancen los 1028 kB se archivará el fichero con el nombre: **"Archive-Microsoft IIS-Configuration%4Operational-[año]-[mes]-[día]-[hora]-[minuto]-[segundo]-[milésima de segundo].evtx".** **Nota:** Estos ficheros deberán ser copiados y eliminados periódicamente para evitar su pérdida y el llenado del disco duro.
63.	El servidor se encuentra configurado con todos los parámetros básicos de seguridad.
64.	Ya puede cerrar todas las consolas abiertas y eliminar los archivos utilizados durante el paso a paso.
65.	Finalmente, inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en un Controlador de Dominio.

66.	En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.  *Ilustración 135 - Administración de directivas de grupo*
67.	Despliegue el panel izquierdo hasta llegar a la OU “Domain Controllers”.  *Ilustración 136 - OU Domain Controllers*
68.	Despliegue dicha OU, haga clic derecho sobre el GPO “CCN-STIC-570A25_DC_AnexoA – ADMX (Nivel de Clasificación)”, y seleccione “Editar”.  *Ilustración 137 - Edición ADMX 570A25*
69.	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 138 - Políticas de PowerShell*
70.	Haga doble clic sobre la política “Activar la ejecución de scripts”.

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

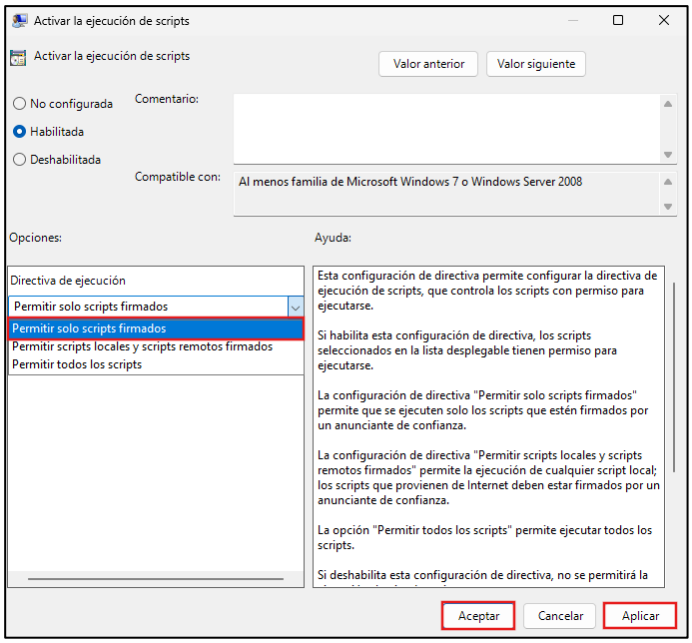


Ilustración 139 - Selección de "Permitir solo scripts firmados"

ANEXO A.2. CONFIGURACIONES ADICIONALES DE SEGURIDAD

ANEXO A.2.1. GESTIÓN DE PERMISOS DEL SITIO WEB

Se recomienda realizar una gestión lo más severa posible de permisos de los sitios web, por lo que debería configurar el sitio para limitar el acceso a exclusivamente a aquellos usuarios autorizados.

Editará los permisos de la carpeta física del sitio para limitar el acceso en primer nivel. Va a suponer, a modo de ejemplo, que este sitio va a ser exclusivamente para administradores.

Nota: Se va a utilizar un sitio web a modo de ejemplo llamado “prueba”.

Paso	Descripción
1.	Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en el Servidor IIS.

2.	Sobre la barra de búsqueda, escriba “Administrador de Internet Information Services (IIS)”.

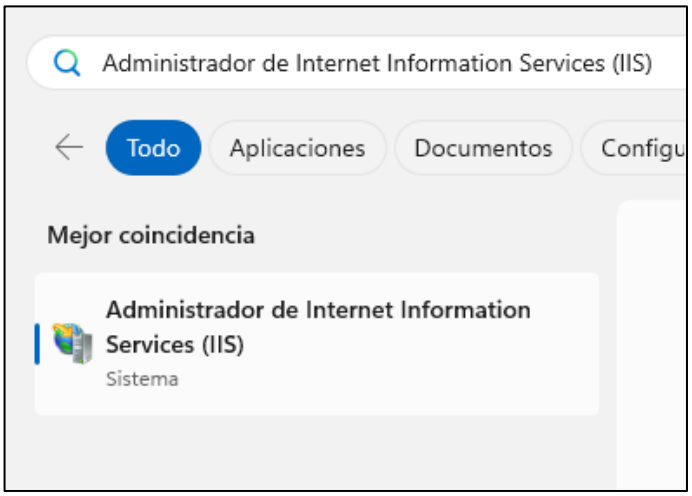


Ilustración 140 - Administrador de Internet Information Sevices

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

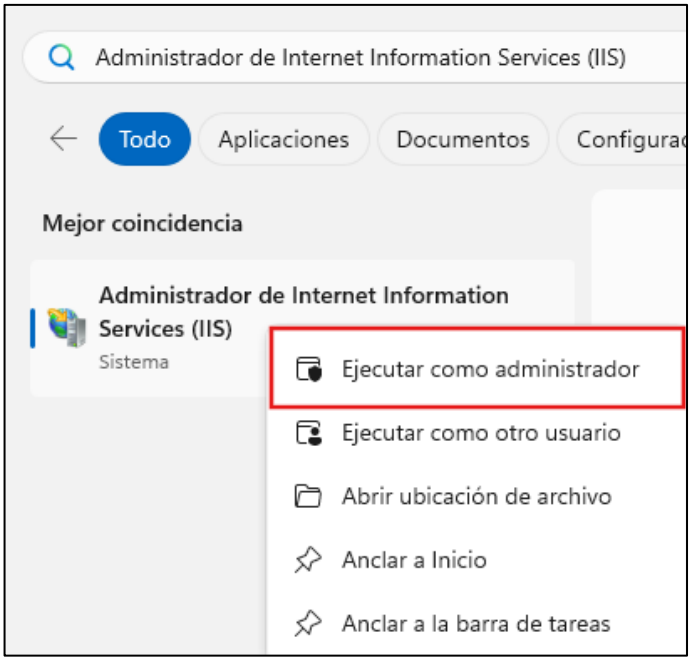
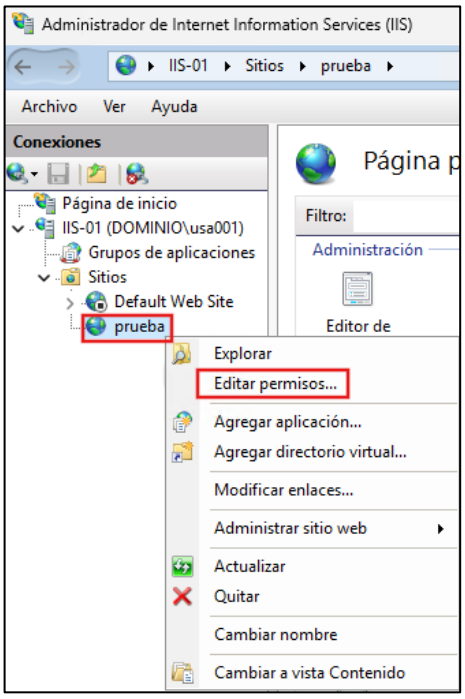
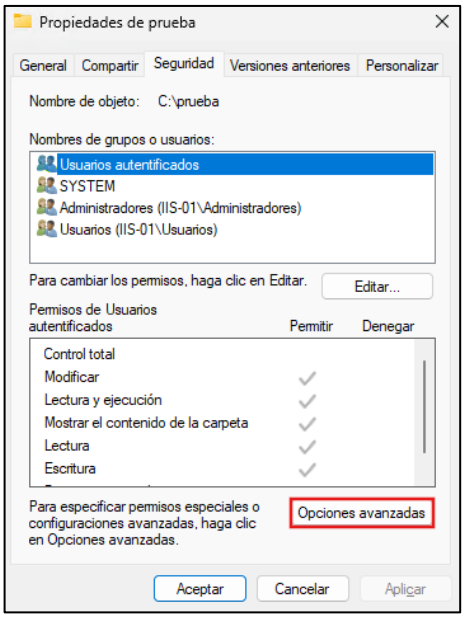
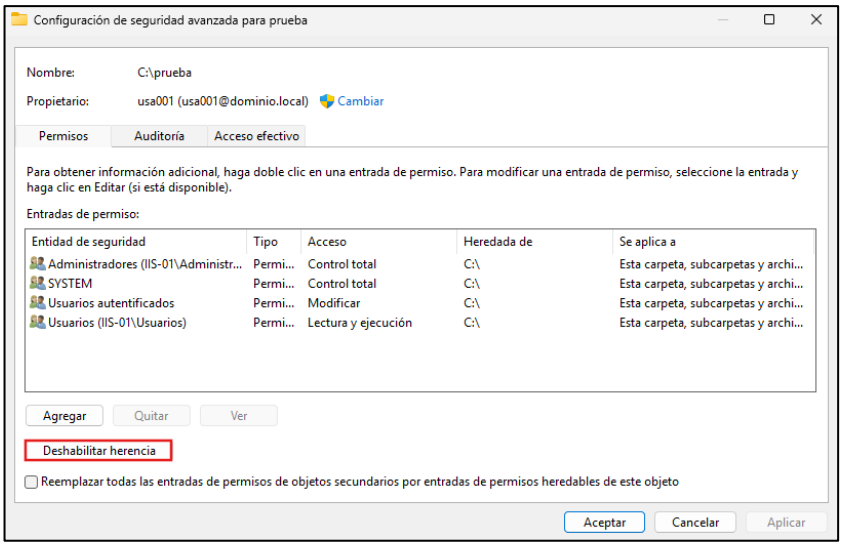
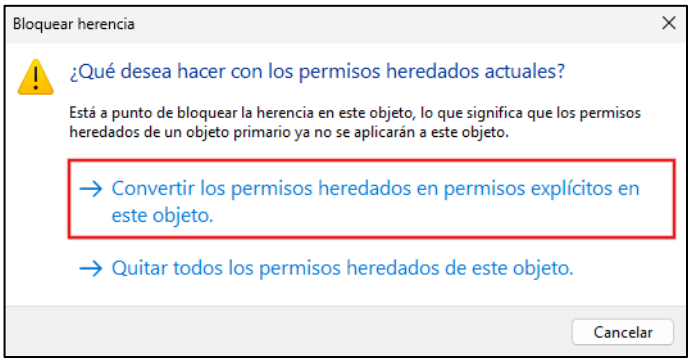


Ilustración 141 - Ejecutar modo administrador

4.	En el árbol de conexiones, sitúese sobre el nodo **"Administrador de Internet Information Services (IIS) > [nombre_del_servidor]"** y en el menú contextual del sitio web "prueba" seleccione "Editar permisos…".  *Ilustración 142 - Editar permisos*
5.	Revise los permisos y verá que para dejar los requeridos tiene que quitar algunos a varios usuarios y grupos. Por ello, edite los permisos seleccionando "Opciones avanzadas".  *Ilustración 143 - Seguridad directorio*

6.	Observe que los permisos de la carpeta son los heredados de la carpeta raíz (en este caso coincide con la raíz del disco "C:\", pero deshabilitará esa característica.  *Ilustración 144 - Deshabilitar herencia*
7.	Como quiere dejar una lista de permisos final parecida a los permisos heredados, indique "Convertir los permisos heredados en permisos explícitos en este objeto".  *Ilustración 145 - Aceptar mensaje de información*

8.	Proceda a eliminar los permisos que no desea, los de usuarios no administradores y al usuario de la instalación.

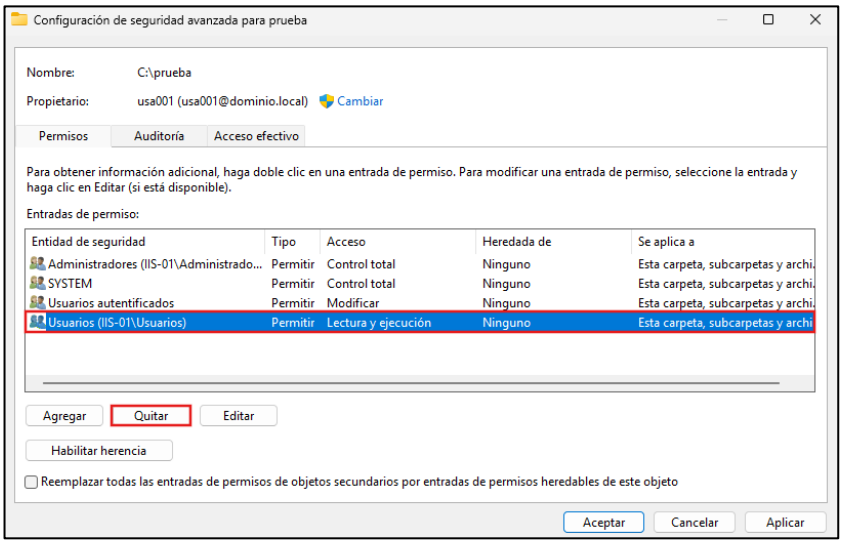


Ilustración 146 - Quitar usuarios no deseados

ANEXO A.2.2. MODIFICACIÓN DEL PUERTO TCP DE SERVICIO DE UN SITIO WEB

Los sitios web utilizan habitualmente puertos predeterminados conocidos por todos los navegadores, por lo que no es necesario incorporarlos en la URL. Para HTTP se utiliza el 80 y para HTTPS el 443. Tanto en un caso como en el otro se puede requerir cambiarlos por motivos de producción o por seguridad.

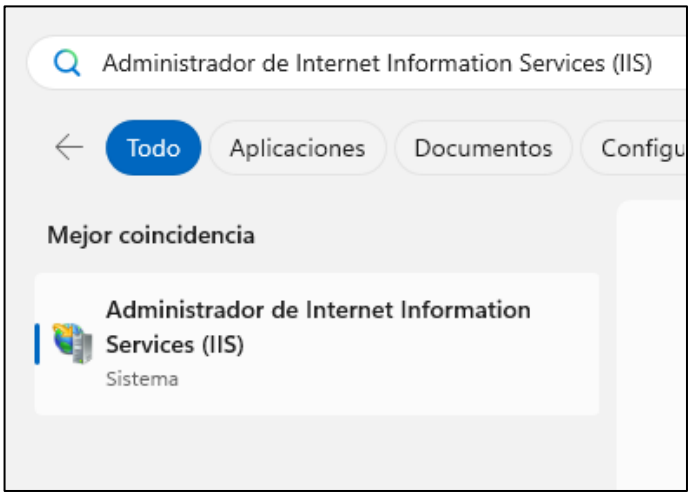
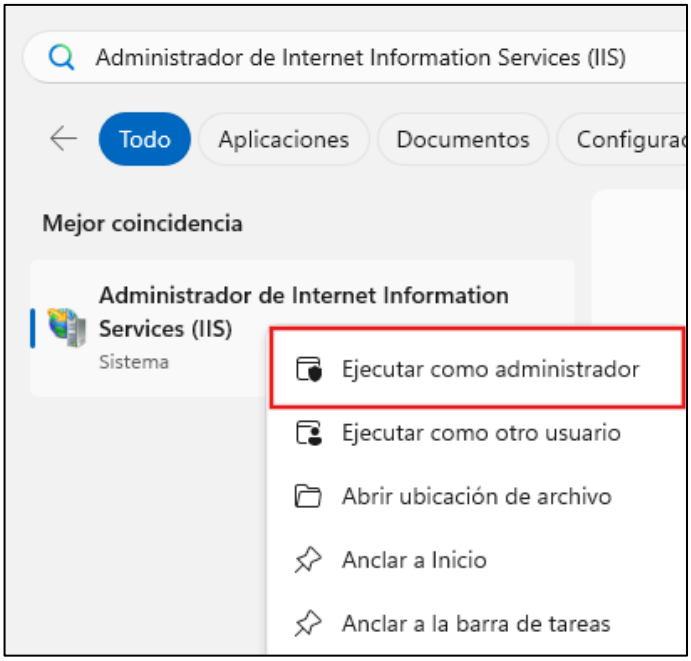
Utilizar un puerto distinto del 80 para la navegación de un sitio web proporciona un nivel de seguridad adicional, si bien muy básico, ya que exige que el usuario tenga que conocerlo para poder conectar con el servidor, además muchos firewalls o sistemas de protección podrían tener "abierto" por defecto el puerto 80, pero difícilmente ocurrirá eso con uno elegido de forma aleatoria.

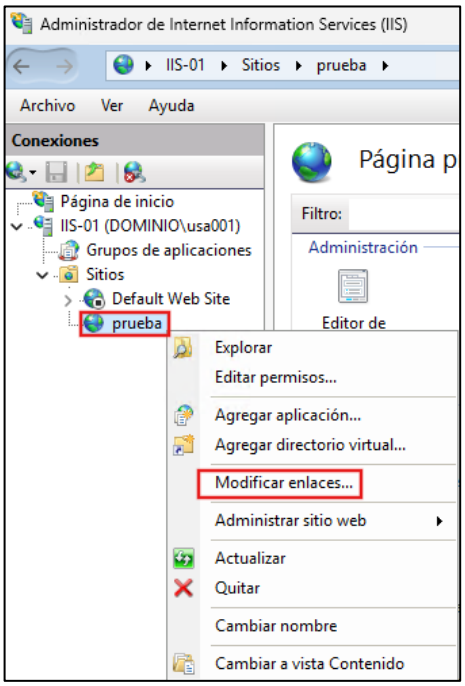
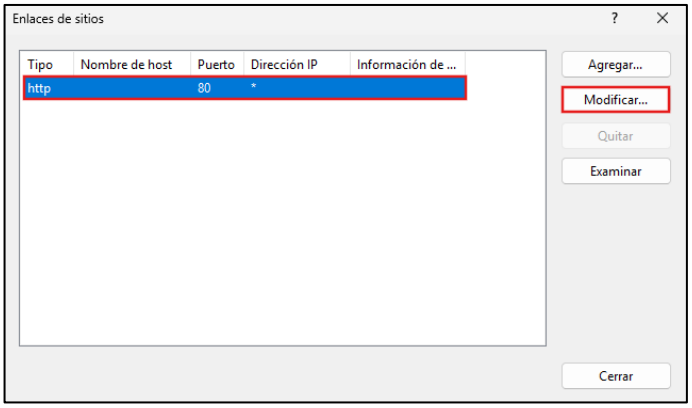
Va a cambiar el puerto de publicación de un sitio instalado en el servidor IIS 10 y comprobar que funcione correctamente.

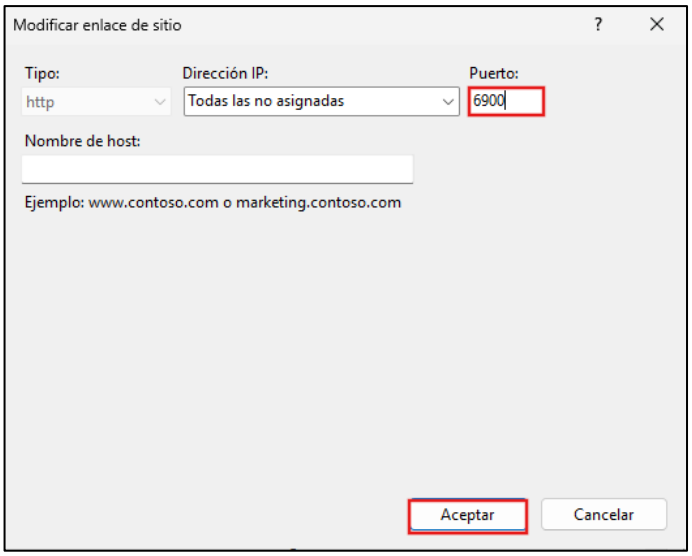
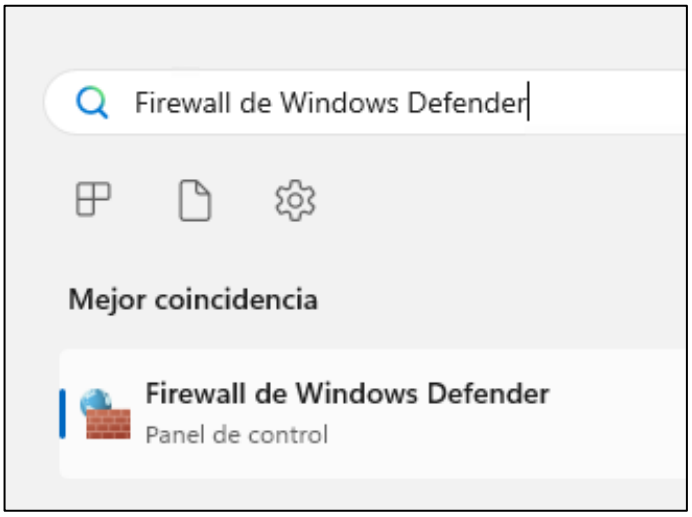
Nota: Se debe seleccionar un puerto por encima del 1023 y por debajo del 49152.

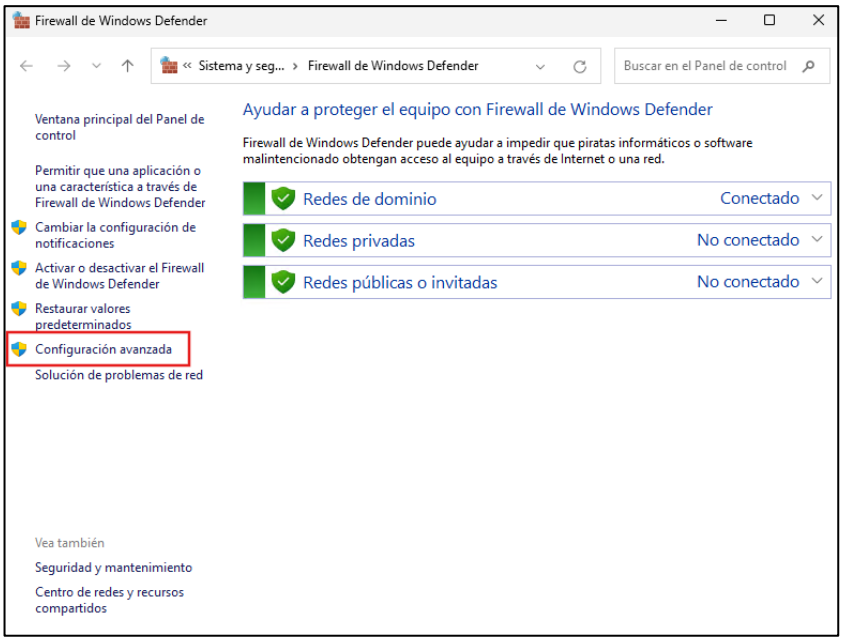
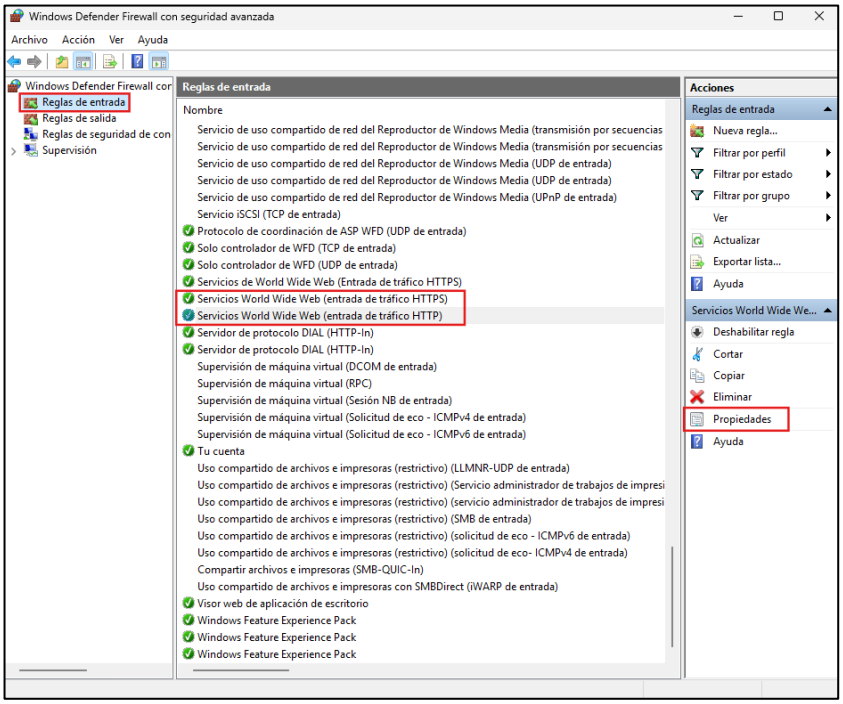
El ejemplo que va a completar es en el entorno de prueba, el cual tiene un sitio web conocido como "prueba" que publica en el puerto 80, pero se quiere modificar al 6900.

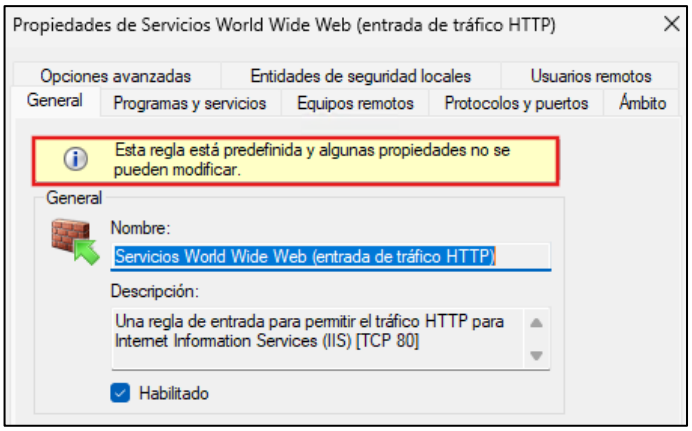
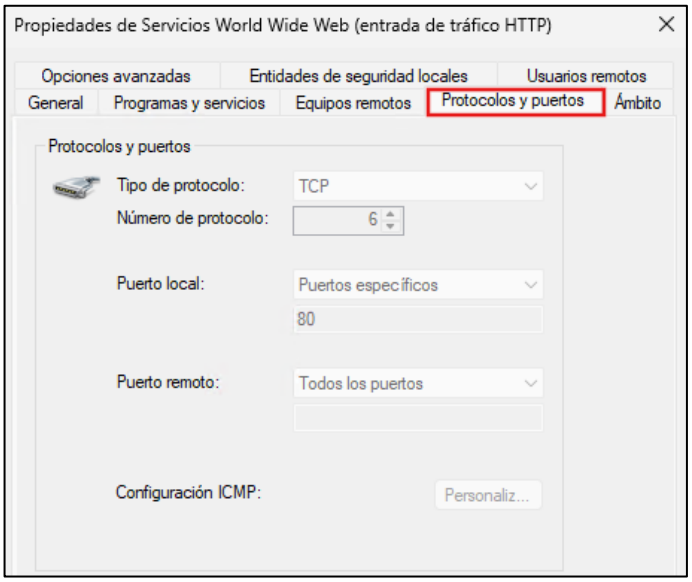
Paso	Descripción
1.	Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en el Servidor IIS.

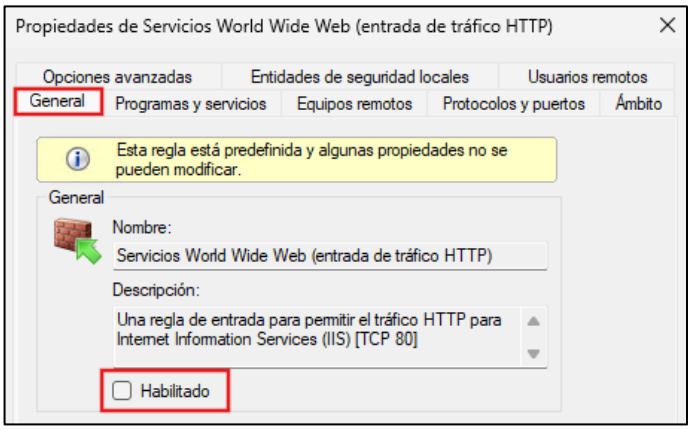
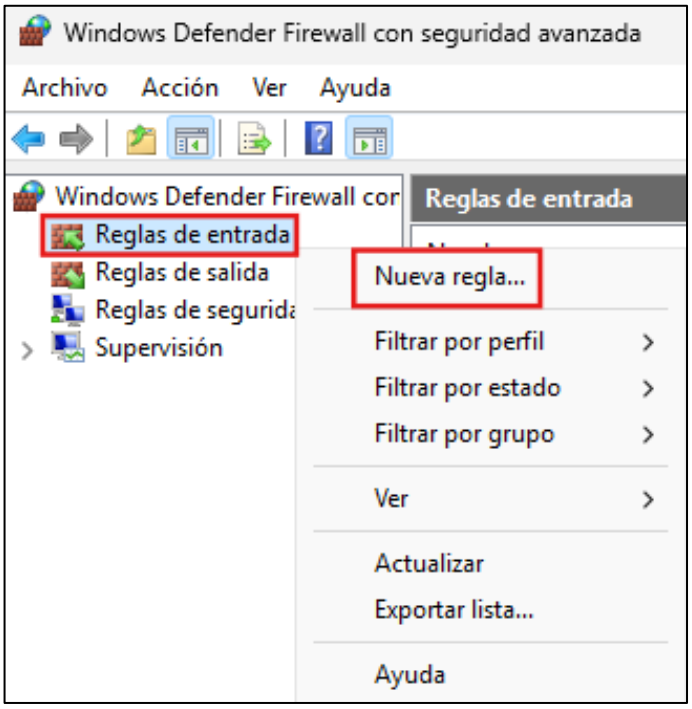
2.	Sobre la barra de búsqueda, escriba “Administrador de Internet Information Services (IIS)”.  *Ilustración 147 - Administrador de Internet Information Sevices*
3.	Haga clic derecho y seleccione “Ejecutar como administrador”.  *Ilustración 148 - Ejecutar modo administrador*

4.	En el árbol de conexiones, sitúese sobre el nodo “Administrador de Internet Information Services (IIS) > [nombre_del_servidor]” y en el menú contextual del sitio web “prueba” seleccione “Modificar enlaces…”.  *Ilustración 149 - Modificar enlaces*
5.	En la ventana emergente aparecerá el puerto en el que actualmente escucha peticiones el sitio web. Marque la línea y presione el botón “Modificar…”.  *Ilustración 150 - Modificar enlace del sitio*

6.	Ahora puede poner el puerto real de escucha, 6900, y que será operativo desde la aceptación. Acepte esta ventana y cierre “Enlaces de sitios”.  *Ilustración 151 - Modificar puerto*
7.	Sobre la barra de búsqueda, escriba “Firewall de Windows Defender” y ejecútelo.  *Ilustración 152 - Firewall de Windows Defender*

8.	En la ventana seleccione “Configuración avanzada”.  *Ilustración 153 - Configuración avanzada*
9.	En el árbol, seleccione “Firewall de Windows con seguridad avanzada” > Reglas de entrada”. En la lista ordenada que aparece puede ver, en la parte baja, que existen dos reglas relacionadas con el servidor web.  *Ilustración 154 - Reglas de entrada*

10.	Si abre las propiedades de, por ejemplo, la primera de las reglas puede ver que son reglas predeterminadas y que, como avisa, no todos los parámetros son modificables.  *Ilustración 155 - Aviso de regla de entrada*
11.	En la pestaña “Protocolos y puertos” puede ver que uno de los parámetros que no se puede modificar es el puerto.  *Ilustración 156 - Protocolos y puertos*

12.	Si el puerto 80 no se utilizará para servicios web, deshabilite la regla correspondiente en el firewall.  *Ilustración 157 - Deshabilitar regla* **Nota:** Esta decisión debe Ud. tomarla teniendo en consideración la configuración definitiva que va a tener el servidor.
13.	Ahora creará la regla que permita publicar por el puerto 6900, como se había seleccionado, a modo de ejemplo. En el árbol del firewall, sobre “Reglas de entrada”, y en el menú contextual opte por “Nueva regla…”.  *Ilustración 158 - Nueva regla*

14.	El asistente le guiará para la creación de la regla ajustándose lo más posible al futurible uso de la misma. En este caso, se ha de seleccionar la opción “Puerto” y pulsar sobre “Siguiente >”.

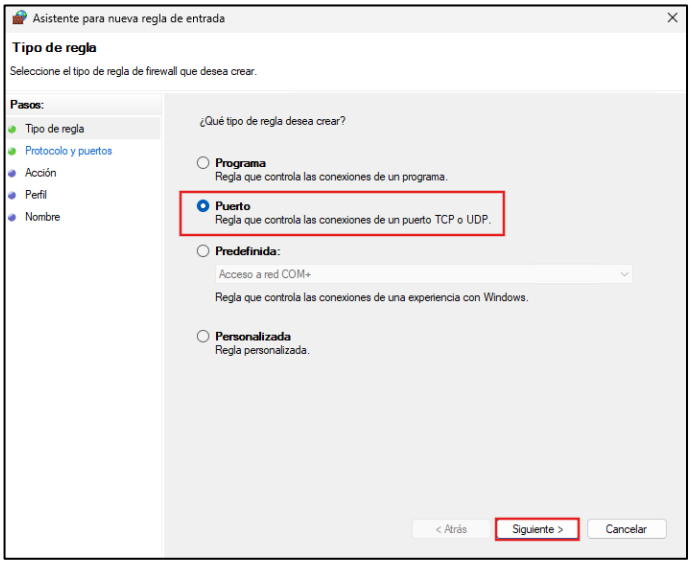


Ilustración 159 - Tipo de regla

15.	En la siguiente ventana, “Protocolo y puerto”, introduzca el valor del puerto, 6900 y pulse sobre “Siguiente >”.

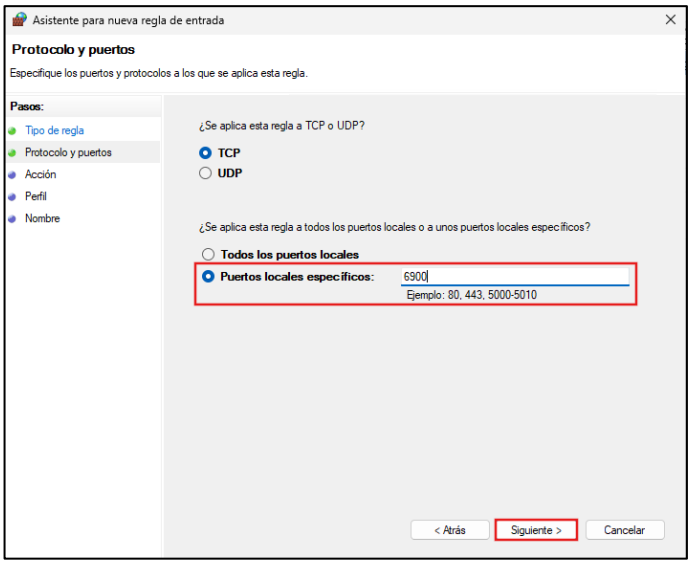
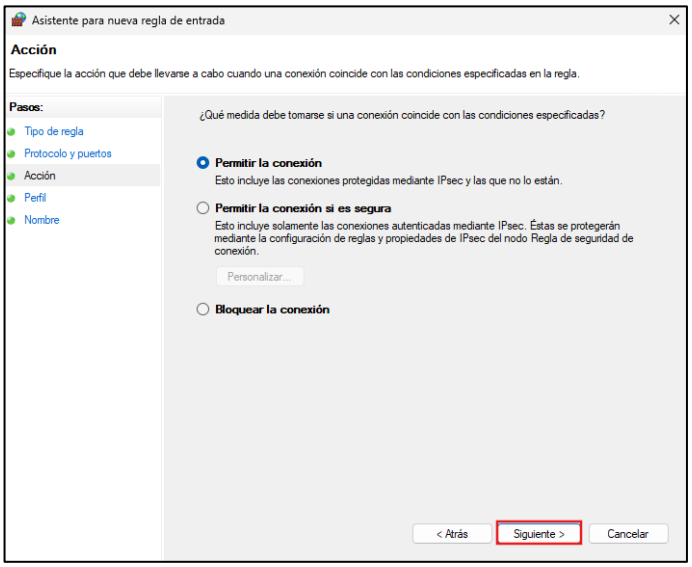
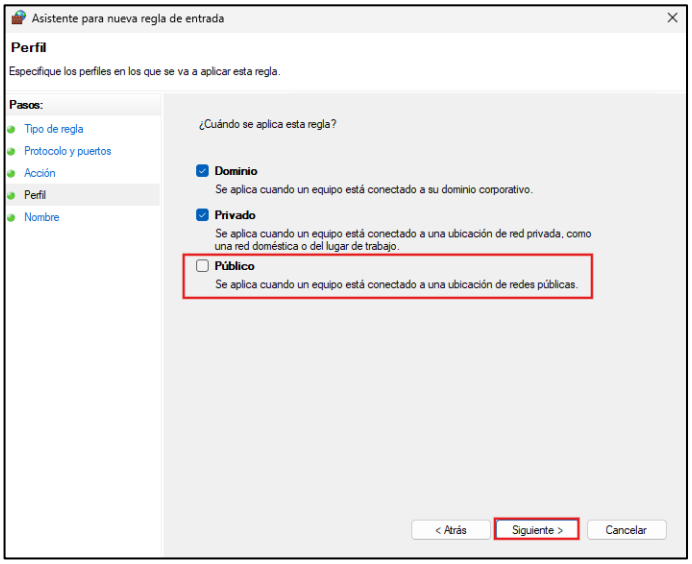
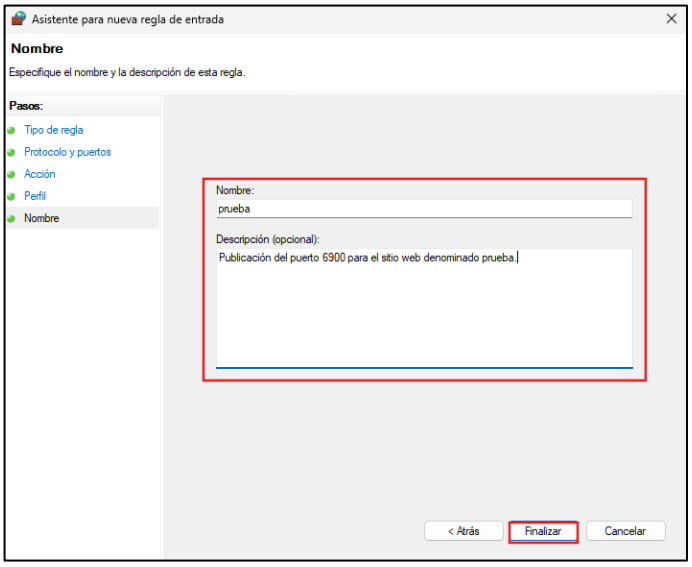
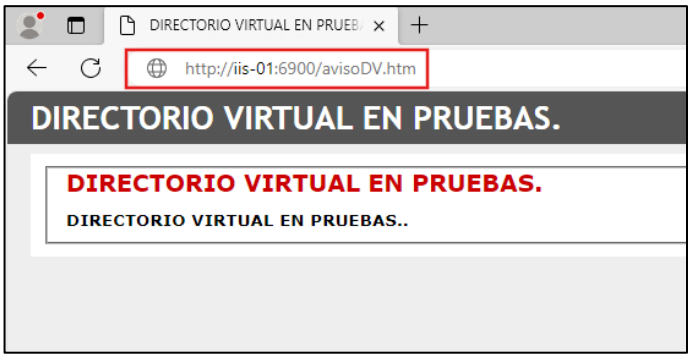


Ilustración 160 - Puerto

16.	En la ventana “Acción” no modifique ningún parámetro, por lo que debe pulsar sobre “Siguiente >”.  *Ilustración 161 - Permitir la conexión del puerto*
17.	En el perfil puede filtrar el origen de las conexiones. Este filtrado es adicional al que podía establecer en el propio IIS. Aunque se consideren redundantes, debería contemplar como una buena opción configurar ambos. Ya que el entorno de instalación es el de un dominio o bosque donde se integran los servidores y clientes, elimine la opción “Público” y pulse sobre “Siguiente >”.  *Ilustración 162 - Selección de perfiles*

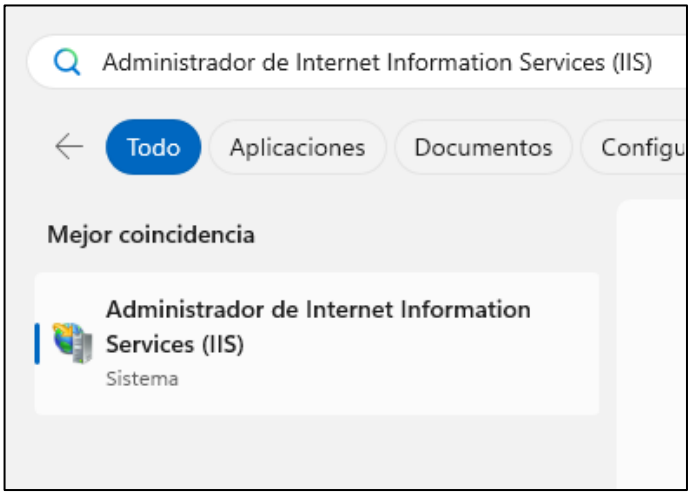
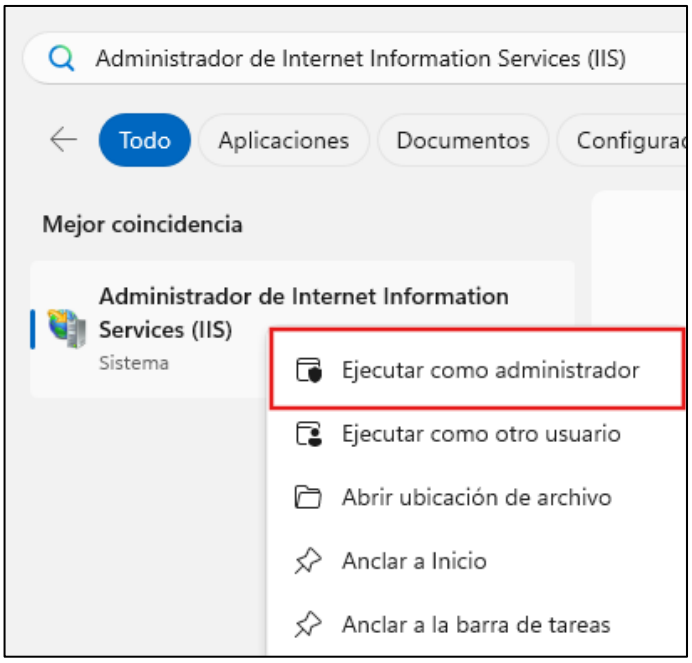
18.	Por último, establezca un nombre descriptivo y claro, así como una descripción. Se considera una buena práctica realizar descripciones adecuadas, e incluso fechadas y firmadas, para poder hacer un seguimiento de las mismas. Pulse sobre “Finalizar” para acabar la definición de la regla.  *Ilustración 163 - Nombre de la regla*
19.	Puede probar el acceso desde otro equipo introduciendo la URL en el navegador.  *Ilustración 164 - Prueba del URL* **Nota:** Se ha utilizado un archivo .htm a modo de prueba para la realización de la guía.

ANEXO A.2.3. CREACIÓN DE SITIO WEB HTTPS

Crear un sitio web con conexiones HTTPS se considera una práctica recomendable en casi todas las ocasiones, desde comienzos de la primera década del siglo XXI se utiliza de forma habitual en sitios donde hay ciertos datos a proteger y desde la segunda década se ha establecido en muchos sitios populares para proteger a los usuarios de los posibles capturadores de navegación y otras prácticas dañinas.

Los inconvenientes que podrían decantarnos por la no activación serían: mayor carga administrativa, bajada del rendimiento de los servidores y mayor dificultad de seguimiento de las acciones de los usuarios.

En este ejemplo hará que el sitio web “prueba” sea servido de forma segura con HTTPS y que sea el único protocolo posible.

Paso	Descripción
1.	Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en el Servidor IIS.
2.	Sobre la barra de búsqueda, escriba “Administrador de Internet Information Services (IIS)”.  *Ilustración 165 - Administrador de Internet Information Sevices*
3.	Haga clic derecho y seleccione “Ejecutar como administrador”.  *Ilustración 166 - Ejecutar modo administrador*

4.	En el árbol de conexiones, sitúese sobre el nodo “Administrador de Internet Information Services (IIS) > [nombre_del_servidor]”.

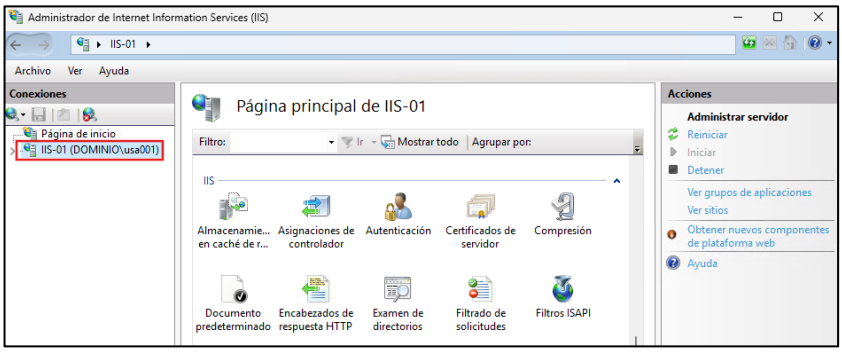


Ilustración 167 - Página principal de IIS

5.	Antes de proceder a la “Configuración de SSL” de un sitio web determinado o de habilitar enlaces sobre HTTPS necesita un certificado que asegure que se pueden intercambiar comunicaciones entre servidor y cliente de forma cifrada. Para ellos abra “Certificados de servidor” del servidor.

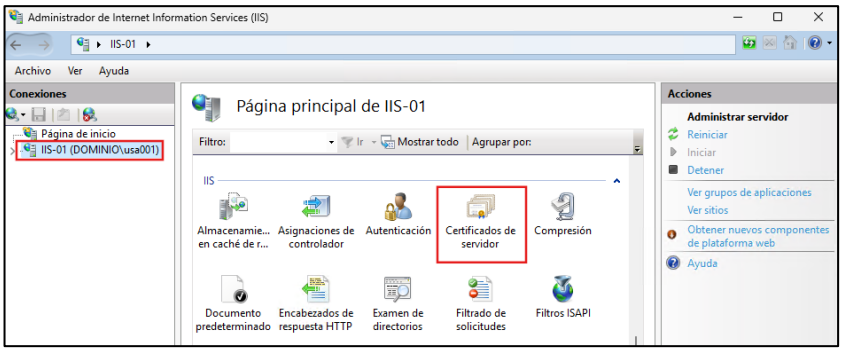


Ilustración 168 - Certificados de servidor

6.	En la página de certificados de servidor se le muestran aquellos que pudiera tener ya alojados y las acciones principales que se pueden realizar. En este caso va a seleccionar un “certificado autofirmado”, que minimiza las tareas administrativas y que para dentro de un dominio es una solución aceptable, aunque siempre se deberá tender a utilizar certificados del dominio para la intranet. Seleccione “Crear certificado autofirmado…”.

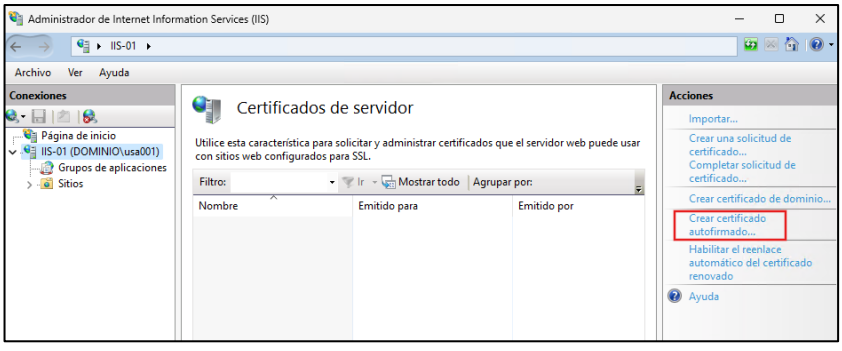
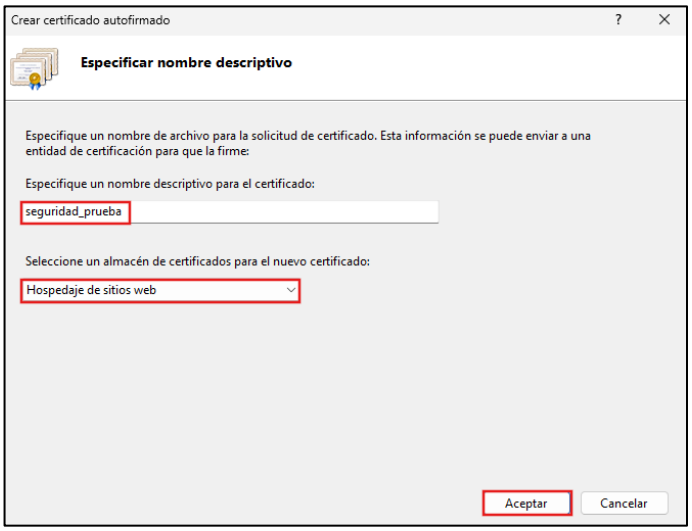
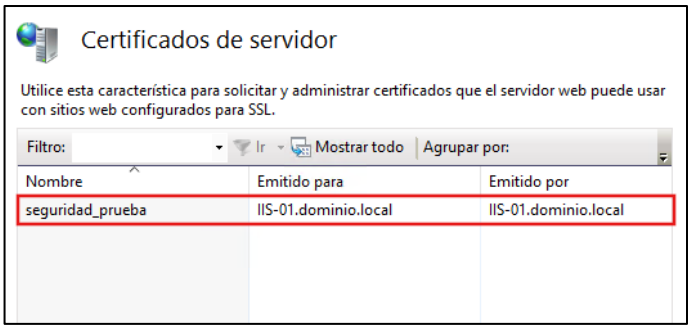
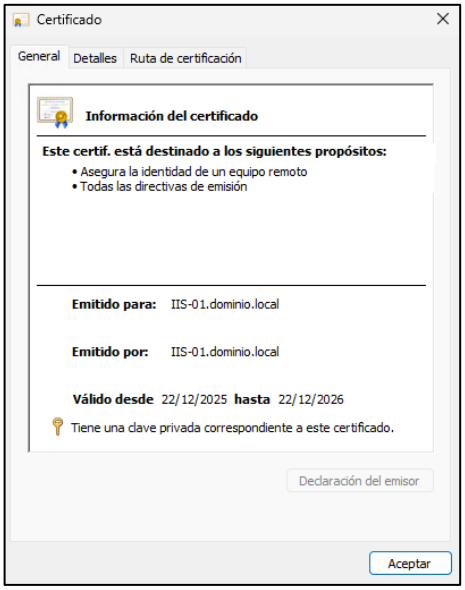
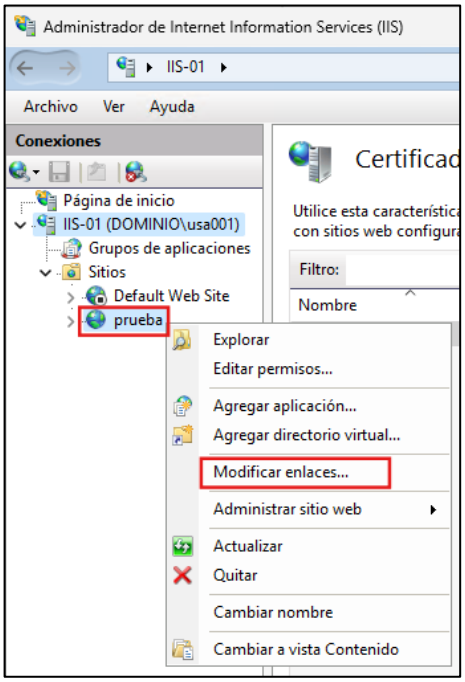
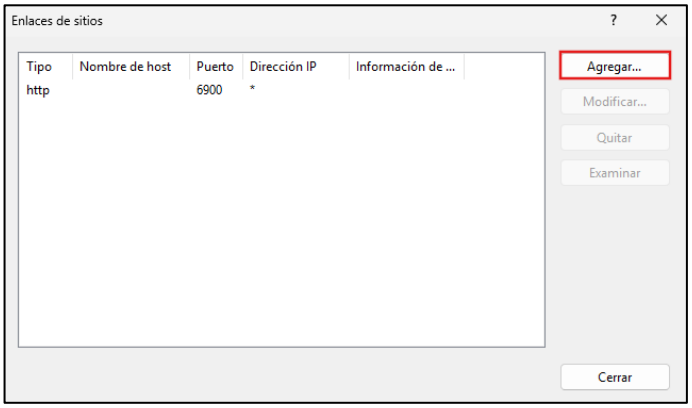
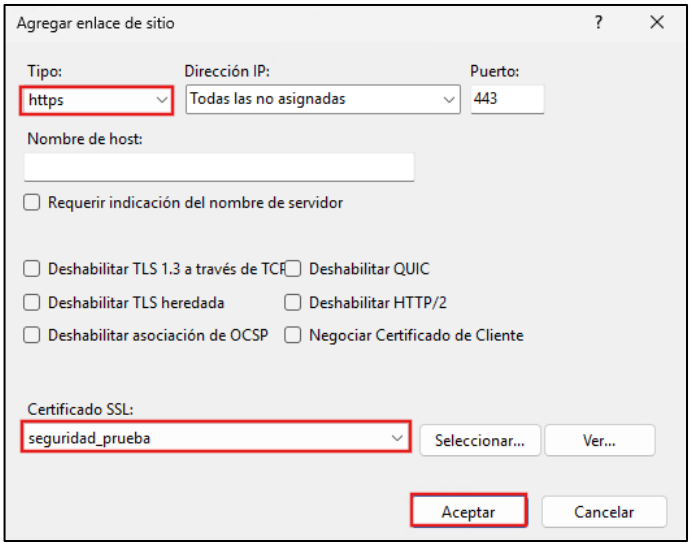
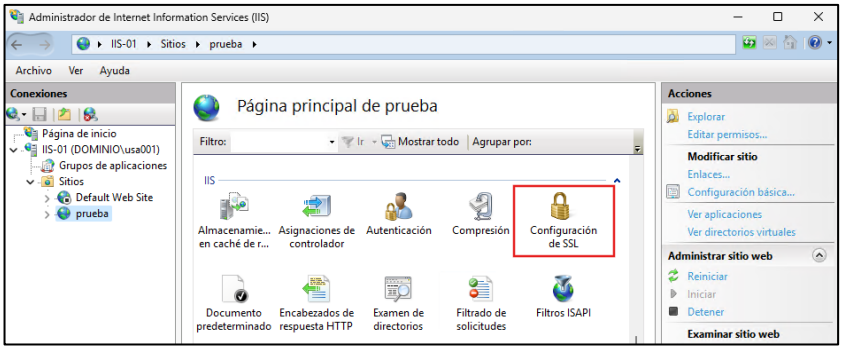
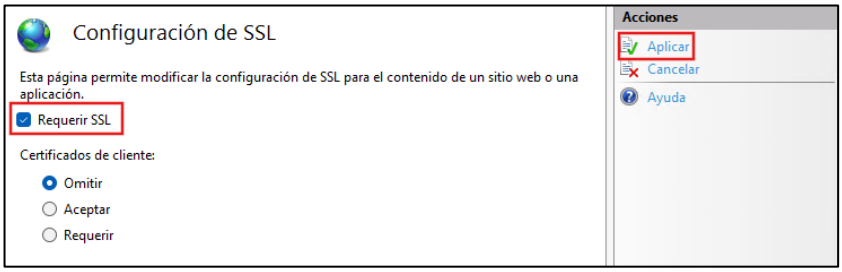


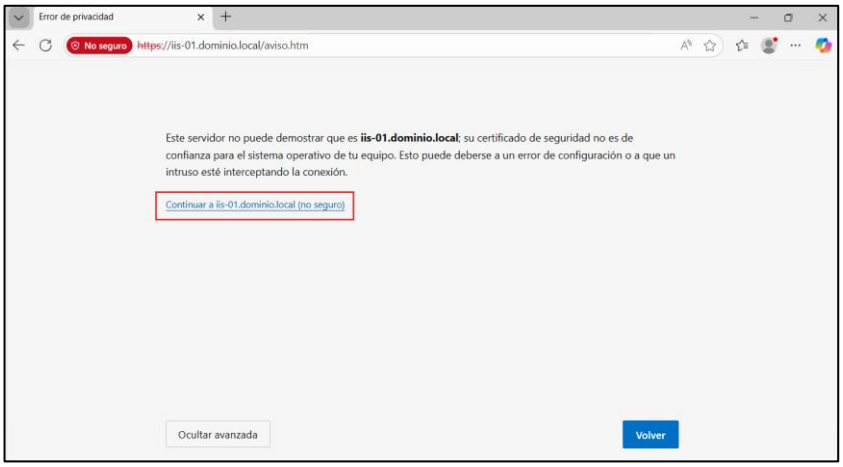
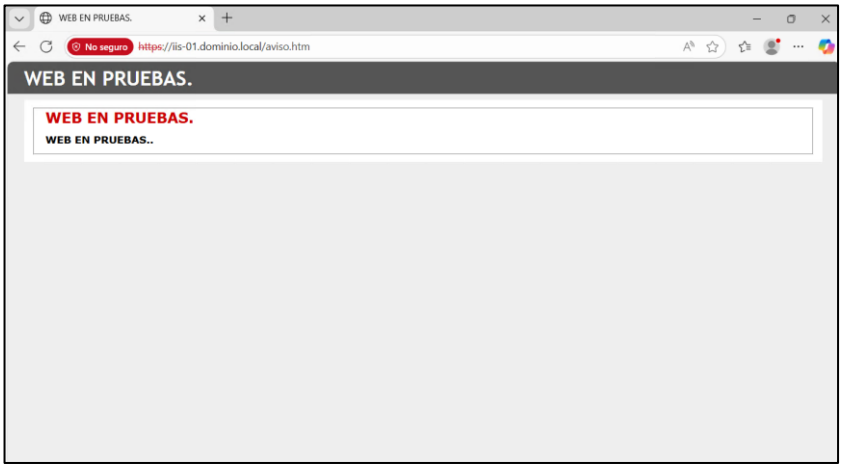
Ilustración 169 - Crear certificado autofirmado

7.	Asigne el nombre “seguridad_prueba” y seleccione la opción “Hospedaje de sitios web”. Posteriormente, pulse “Aceptar”.  *Ilustración 170 - Especificar nombre descriptivo*
8.	Aparecerá en la lista de certificados disponibles.  *Ilustración 171 - Certificados de servidor*

9.	Haciendo doble clic sobre él, se abre la ventana del certificado y muestra los datos. Destacar: - Validez: 1 año. - Clave pública: RSA (2048 bits). - Clave privada: incluida (lo que le permite utilizarlo para el intercambio SSL).  *Ilustración 172 - Información del certificado*
10.	En el árbol de conexiones seleccione el sitio web que quiere configurar y sobre él abra el menú contextual, con el botón derecho del ratón, y marque “Modificar enlaces…”.  *Ilustración 173 - Modificar enlace*

11.	Añada un nuevo enlace pulsando sobre “Agregar…”.  *Ilustración 174 - Agregar enlace*
12.	Seleccione el tipo como “https” y el certificado recién creado y el certificado autofirmado recién creado. Pulse sobre “Aceptar” para aplicar cambios.  *Ilustración 175 - Selección del certificado*

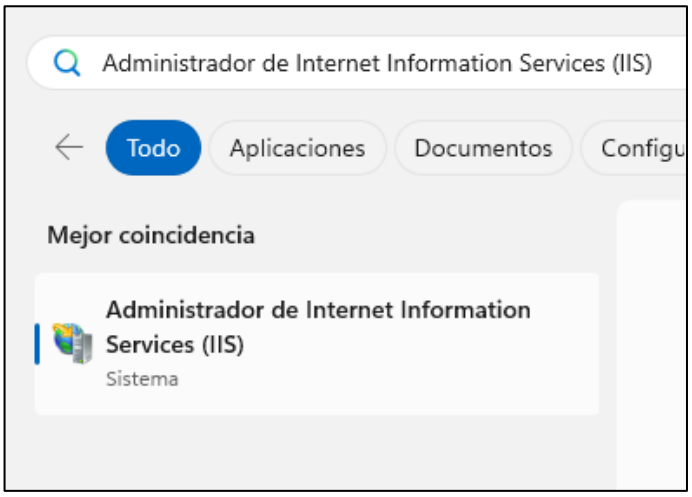
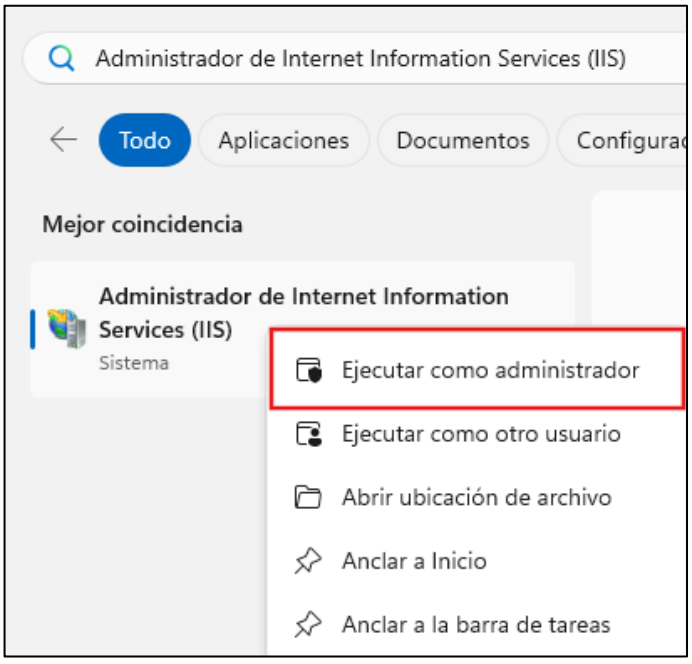
13.	Los enlaces del sitio “prueba” quedarán como se muestra en la imagen. Pulse “Cerrar”.  *Ilustración 176 - Enlaces del sitio*
14.	Ahora abra la opción “Configuración de SSL” del sitio web.  *Ilustración 177 - Configuración de SSL*
15.	Fuerce el requerir SSL y deje en “Omitir” los certificados de cliente. Por último, marque “Aplicar”.  *Ilustración 178 - Requerimiento de SSL*
16.	Ahora ha quedado configurado el acceso de forma segura en exclusiva, aunque tenga dos escuchas, una en un puerto HTTP y otra en HTTPS. En el servidor debe asegurarse que tiene la regla de firewall adecuada ya que ha utilizado el puerto (443) y la regla de firewall predeterminados.

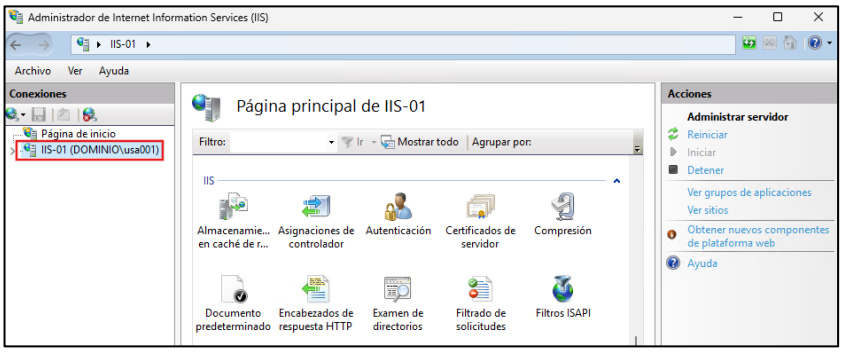
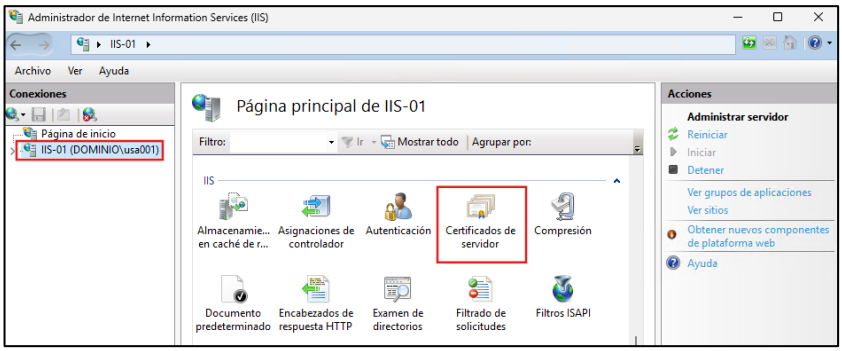
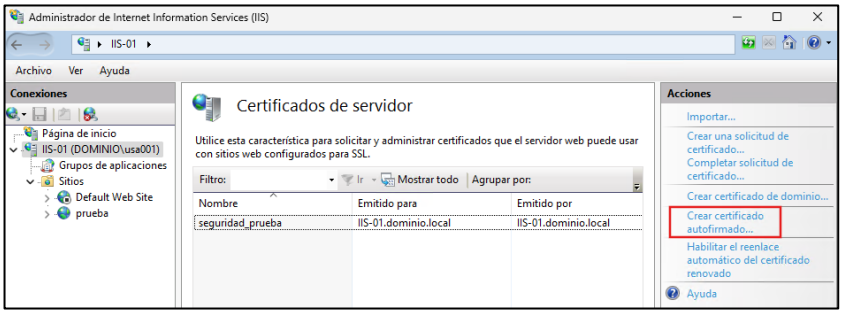
17.	Compruebe que el acceso vía HTTPS está operativo desde un navegador. Utilice la URL: https://iis-10.dominio.local/aviso.htm (se utiliza "localhost" cuando la prueba se hace desde un navegador del propio servidor IIS 10). Al abrir será avisado de falta de confianza en el certificado, y durante la navegación aparecerá un aviso constante al respecto, como verá más adelante. Si la prueba de navegación se hace desde el propio servidor IIS no aparecerán avisos de falta de confianza en el certificado, al ser el del equipo.  *Ilustración 179 – Aviso de URL*
18.	Ahora se despliega la web de pruebas, confirmando que el acceso por HTTPS está operativo.  *Ilustración 180 - Comprobación de URL*

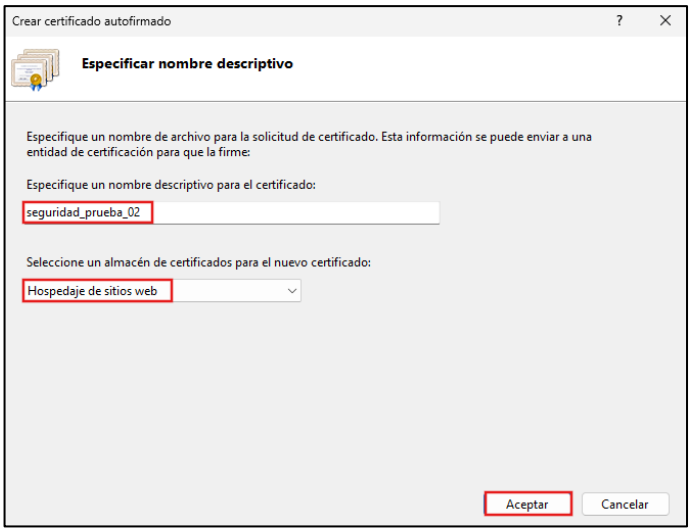
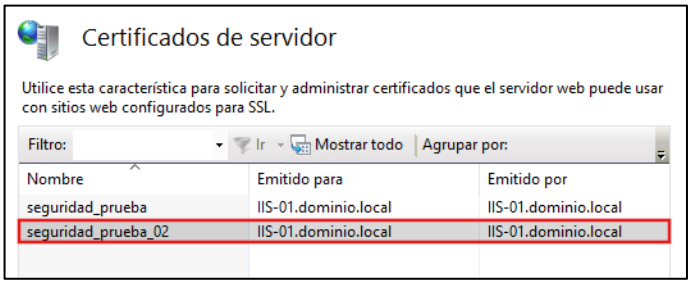
ANEXO A.2.4. PROCEDIMIENTO DE RENOVACIÓN DE CERTIFICADO EN SERVIDOR WEB

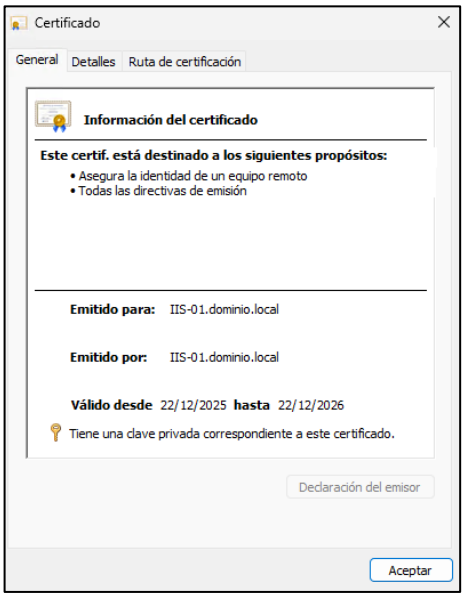
A continuación, se muestran los pasos necesarios para que, en caso de no disponer de una infraestructura de clave pública (PKI) o haber tomado la decisión de continuar con el certificado autofirmado predeterminado, este se pueda sustituir sin problemas

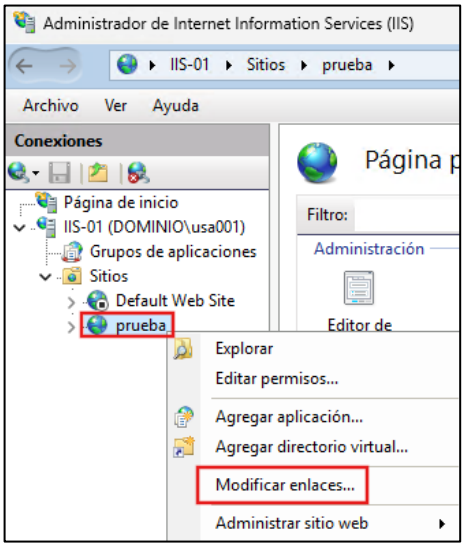
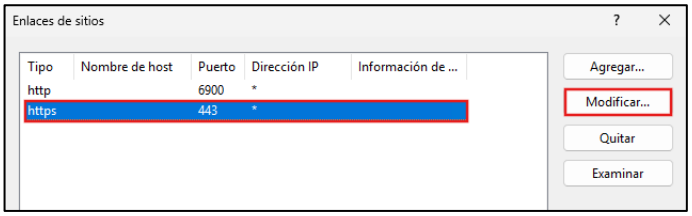
pasado su tiempo de validez, aunque la recomendación es la sustitución antes de la fecha de caducidad del certificado para evitar problemas de continuidad del servicio que preste el servidor.

Paso	Descripción
1.	Inicie sesión con un usuario perteneciente al grupo Admins. De Dominio en el Servidor IIS.
2.	Sobre la barra de búsqueda, escriba “Administrador de Internet Information Services (IIS)”.  *Ilustración 181 - Administrador de Internet Information Sevices*
3.	Haga clic derecho y seleccione “Ejecutar como administrador”.  *Ilustración 182 - Ejecutar modo administrador*

4.	En el árbol de conexiones, sitúese sobre el nodo “Administrador de Internet Information Services (IIS) > [nombre_del_servidor]”.  *Ilustración 183 - Página principal de IIS*
5.	Antes de proceder a la “Configuración de SSL” de un sitio web determinado o de habilitar enlaces sobre HTTPS necesita un certificado que asegure que se pueden intercambiar comunicaciones entre servidor y cliente de forma cifrada. Para ellos abra “Certificados de servidor” del servidor.  *Ilustración 184 - Certificados de servidor*
6.	En la página de certificados de servidor se le muestran aquellos que pudiera tener ya alojados y las acciones principales que se pueden realizar. En este caso va a “Crear certificado autofirmado…”.  *Ilustración 185 - Crear certificado autofirmado*

7.	Le debe dar un nombre, por ejemplo, “seguridad_prueba_02”. Acepte, lo que finaliza el proceso de creación.  *Ilustración 186 - Especificar nombre descriptivo*
8.	Aparecerá en la lista de certificados disponibles:  *Ilustración 187 - Certificados disponibles*

9.	Haciendo doble clic sobre él, se abre la ventana del certificado y muestra los datos. Destacar: - Validez: 1 año - Clave pública: RSA (2048 bits) Clave privada: incluida (lo que nos permite utilizarlo para el intercambio SSL).  *Ilustración 188 - Información de certificado*
10.	Una vez creado el nuevo certificado podrá utilizarlo para sustituir el certificado autofirmado caducado o con fecha pronta a caducar.

11.	En el árbol de conexiones seleccione el sitio o sitios web y el sitio o sitios FTP que utilizaban el certificado a punto de caducar o recientemente caducado. No existe un procedimiento que pudiera modificar de forma genérica todos los sitios. Sobre el sitio marque “Modificar enlaces…” con el botón derecho del ratón.  *Ilustración 189 - Modificación de enlace*
12.	Abra el enlace existente al puerto 443, y que es el que está utilizando el certificado expirado o a punto de expirar, márquelo para modificar.  *Ilustración 190 - Modificar enlace https*

13.	Seleccione el nuevo certificado y acepte.

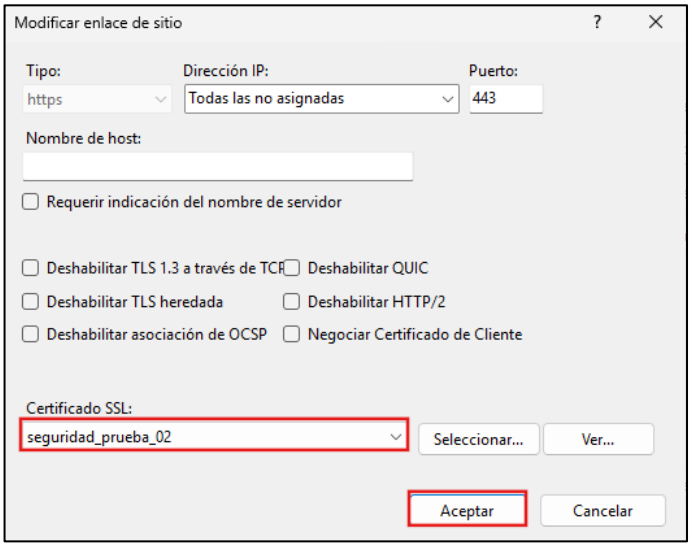


Ilustración 191 - Selección de ceritificado nuevo

PUBLICACIONES DE DEFENSA

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