CCN
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 574

IMPLEMENTACIÓN DEL ENS EN INTERNET INFORMATION SERVICES 10 SOBRE WINDOWS SERVER 2016

DICIEMBRE 2018

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN
centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2018.12.04 11:43:45 +01'00'

NIPO: 083-19-036-1
Fecha de Edición: diciembre de 2018

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

PRÓLOGO

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

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

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

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

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

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

diciembre de 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE INTERNET INFORMATION SERVICES 10 SOBRE MICROSOFT WINDOWS SERVER 2016 8
ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE INTERNET INFORMATION SERVICES 10 SOBRE MICROSOFT WINDOWS SERVER 2016 8
1. APLICACIÓN DE MEDIDAS EN INTERNET INFORMATION SERVICES 10 8
1.1. MARCO OPERACIONAL 9
1.1.1. CONTROL DE ACCESO 9
1.1.2. EXPLOTACIÓN 12
1.2. MEDIDAS DE PROTECCIÓN 14
1.2.1. PROTECCIÓN DE LAS COMUNICACIONES 14
2. RESUMEN Y APLICACIÓN DE MEDIDAS DE IIS 10 SOBRE WINDOWS SERVER 2016 17
ANEXO A.2. CATEGORÍA BÁSICA 18
ANEXO A.2.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 MIEMBROS DEL DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS 18
1. PREPARACIÓN DEL DOMINIO 18
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN 27
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN 28
2.2. GESTIÓN DE PERMISOS RECURSOS WEB 31
2.3. AUTENTICACIÓN SITIO WEB 34
2.4. CERTIFICADOS 36
2.5. AUDITORÍA 39
2.6. DESHABILITAR MODOS DE DEPURACIÓN 41
2.7. IDENTIDADES DEL GRUPO DE APLICACIONES 44
2.8. LIMPIEZA DE METADATOS 46
2.9. SOLUCIONES WAF (WEB APLICATION FIREWALL) 46
ANEXO A.2.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA BÁSICA DEL ENS PARA SERVIDORES IIS 10 SOBRE MICROSOFT WINDOWS SERVER 2016 EN ENTORNO DE DOMINIO 47
1. COMPROBACIONES EN CONTROLADOR DE DOMINIO 47
2. COMPROBACIONES EN SERVIDOR MIEMBRO 49
ANEXO A.2.3. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 INDEPENDIENTES SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS 54
1. CONFIGURACIÓN DE LA SEGURIDAD LOCAL 55
2. CONFIGURACIONES ESPECIFICAS DE LA ORGANIZACIÓN 59
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN 59
2.2. GESTION DE PERMISOS RECURSOS WEB 63

2.3. AUTENTICACIÓN SITIO WEB 66
2.4. CERTIFICADOS 68
2.5. AUDITORÍA 70
2.6. DESHABILITAR MODOS DE DEPURACIÓN 73
2.7. IDENTIDADES DEL GRUPO DE APLICACIONES 75
2.8. LIMPIEZA DE METADATOS 77
2.9. SOLUCIONES WAF (WEB APLICATION FIREWALL) 77
ANEXO A.2.4. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA BÁSICA DEL ENS PARA SERVIDORES IIS 10 SOBRE MICROSOFT WINDOWS SERVER 2016 78
ANEXO A.3. CATEGORÍA MEDIA 82
ANEXO A.3.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 MIEMBROS DEL DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS 82
1. PREPARACIÓN DE DOMINIO 82
2. CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN 91
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN 91
2.2. GESTION DE PERMISOS RECURSOS WEB 95
2.3. AUTENTICACIÓN SITIO WEB 98
2.4. CERTIFICADOS 100
2.5. PROTOCOLOS DE TRANSMISIÓN 103
2.6. AUDITORÍA 104
2.7. FILTRADO DE SOLICITUDES 113
2.8. DESHABILITAR MODOS DE DEPURACIÓN 116
2.9. IDENTIDADES DEL GRUPO DE APLICACIONES 118
2.10. LIMPIEZA DE METADATOS 121
2.11. SOLUCIONES WAF (WEB APLICATION FIREWALL) 121
3. GESTIÓN DE ROLES Y/O CARACTERÍSTICAS DEL SISTEMA 121
3.1. PREPARACIÓN DEL DIRECTORIO ACTIVO 122
3.2. INSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS 128
3.3. DESINSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS 133
3.4. DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO 137
ANEXO A.3.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA MEDIA DEL ENS PARA SERVIDORES IIS 10 SOBRE MICROSOFT WINDOWS SERVER 2016 EN ENTORNO DE DOMINIO 139
1. COMPROBACIONES EN CONTROLADOR DE DOMINIO 139
2. COMPROBACIONES EN SERVIDOR MIEMBRO 141
ANEXO A.3.3. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 INDEPENDIENTES SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS 149
1. CONFIGURACIÓN DE LA SEGURIDAD LOCAL 149

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN 153
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN 154
2.2. GESTIÓN DE PERMISOS RECURSOS WEB 158
2.3. AUTENTICACIÓN SITIO WEB 160
2.4. CERTIFICADOS 162
2.5. PROTOCOLOS DE TRANSMISIÓN 164
2.6. AUDITORÍA 166
2.7. FILTRADO DE SOLICITUDES 174
2.8. DESHABILITAR MODOS DE DEPURACIÓN 177
2.9. IDENTIDADES DEL GRUPO DE APLICACIONES 178
2.10. LIMPIEZA DE METADATOS 181
2.11. SOLUCIONES WAF (WEB APLICATION FIREWALL) 181
3. GESTIÓN DE ROLES Y/O CARACTERÍSTICAS DEL SISTEMA 181
3.1. PREPARACIÓN DEL SERVIDOR INDEPENDIENTE 182
3.2. INSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS 184
3.3. DESINSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS 189
3.4. DESHABILITACIÓN DE UNA DIRECTIVA DE GRUPO LOCAL 192
ANEXO A.3.4. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA MEDIA DEL ENS PARA SERVIDORES IIS 10 SOBRE MICROSOFT WINDOWS SERVER 2016 EN ENTORNO INDEPENDIENTE 195
ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA 202
ANEXO A.4.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 MIEMBROS DE DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS/DIFUSIÓN LIMITADA 202
1. PREPARACIÓN DEL DOMINIO 202
2. CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN 211
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN 211
2.2. GESTION DE PERMISOS RECURSOS WEB 216
2.3. AUTENTICACIÓN SITIO WEB 218
2.4. CERTIFICADOS 221
2.5. PROTOCOLOS DE TRANSMISIÓN 224
2.6. AUDITORÍA 226
2.7. FILTRADO DE SOLICITUDES 235
2.8. DESHABILITAR MODOS DE DEPURACIÓN 238
2.9. IDENTIDADES DEL GRUPO DE APLICACIONES 240
2.10. LIMPIEZA DE METADATOS 242
2.11. SOLUCIONES WAF (WEB APLICATION FIREWALL) 242
3. GESTIÓN DE ROLES Y/O CARACTERÍSTICAS DEL SISTEMA 243
3.1. PREPARACIÓN DEL DIRECTORIO ACTIVO 243
3.2. INSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS 248

3.3. DESINSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS 253
3.4. DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO 257
ANEXO A.4.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA PARA SERVIDORES IIS 10 SOBRE MICROSOFT WINDOWS SERVER 2016 EN ENTORNO DE DOMINIO 259
1. COMPROBACIONES EN CONTROLADOR DE DOMINIO 259
2. COMPROBACIONES EN SERVIDOR MIEMBRO 261
ANEXO A.4.3. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 INDEPENDIENTES SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA 269
1. CONFIGURACIÓN DE LA SEGURIDAD LOCAL 270
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN 274
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN 274
2.2. GESTIÓN DE PERMISOS RECURSOS WEB 279
2.3. AUTENTICACIÓN SITIO WEB 281
2.4. CERTIFICADOS 284
2.5. PROTOCOLOS DE TRANSMISIÓN 287
2.6. AUDITORÍA 289
2.7. FILTRADO DE SOLICITUDES 299
2.8. DESHABILITAR MODOS DE DEPURACIÓN 302
2.9. IDENTIDADES DEL GRUPO DE APLICACIONES 305
2.10. LIMPIEZA DE METADATOS 307
2.11. SOLUCIONES WAF (WEB APLICATION FIREWALL) 307
3. GESTIÓN DE ROLES Y/O CARACTERÍSTICAS DEL SISTEMA 307
3.1. PREPARACIÓN DEL SERVIDOR INDEPENDIENTE 308
3.2. INSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS 311
3.3. DESINSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS 315
3.4. DESHABILITACIÓN DE UNA DIRECTIVA DE GRUPO LOCAL 319
ANEXO A.4.4. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA PARA SERVIDORES IIS 10 SOBRE MICROSOFT WINDOWS SERVER 2016 EN UN ENTORNO INDEPENDIENTE 322

ANEXO A. CONFIGURACIÓN SEGURA DE INTERNET INFORMATION SERVICES 10 SOBRE MICROSOFT WINDOWS SERVER 2016

ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE INTERNET INFORMATION SERVICES 10 SOBRE MICROSOFT WINDOWS SERVER 2016

1. APLICACIÓN DE MEDIDAS EN INTERNET INFORMATION SERVICES 10

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación de Internet Information Services 10 sobre servidores con Microsoft Windows Server 2016 y que les sea de aplicación el ENS, se establecerán a través de la presente guía las condiciones necesarias de aplicación. Estas se materializarán bien en la aplicación de plantillas de seguridad o bien en procedimientos para garantizar la seguridad, cuando así se demande. En este último caso, por ejemplo, para la segregación de roles, se detallarán procedimientos y condiciones que deberá aplicar un operador de una organización para hacerlas efectivas.

Nota: Tenga en cuenta que en el caso de una red clasificada que ha sido categorizada como Difusión Limitada se hará usó de la aplicación de medidas de seguridad descritas en el "ANEXO A.4 CATEGORÍA ALTA / DIFUSIÓN LIMITADA".

La aplicación de medidas de seguridad atenderá a las siguientes condiciones de implantación de infraestructuras:

a) Aplicación de seguridad en el entorno de Internet Information Services 10 sobre Microsoft Windows Server 2016 que pueda dar soporte a la organización y sobre el que se asientan muchos de los activos tecnológicos de dicha organización. Será, además, el mecanismo empleado para conducir la centralización y gestión de la seguridad.

b) Aplicación de seguridad en servidores miembro de dominio que sustentarán los diferentes servicios que prestara la organización, sujetos al RD 3/2010 y que se encontrarán implementados con Microsoft Windows Server 2016 implementados siguiendo la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016.

Para el análisis y desarrollo de las plantillas a aplicar, así como las tareas administrativas que sean necesarias para el cumplimiento de las medidas dispuestas en el ENS, se tienen en consideración los propios elementos técnicos que aporta Microsoft para Internet Information Services 10, así como otras medidas que puedan ser fácilmente aplicables mediante condiciones de seguridad válidas. Por ejemplo, todas aquellas medidas que puedan ser aplicadas a través de objetos de políticas de grupo (GPO) o las innatas a la gestión del sistema o al propio Directorio Activo, como la asignación de permisos para la segregación de roles y funciones.

Esta guía, por tanto, no referenciará aquellas medidas que, aunque sean de aplicación y de obligado cumplimiento, no sean nativas al sistema operativo o las funcionalidades que el propio rol pueda aportar. Por ejemplo, aunque es condición indispensable la implementación de un antivirus en los servidores, se establece que esta medida atiende a un criterio general de la organización y que, no siendo algo que pueda aportar el propio sistema operativo, se encontrará excluido del análisis e implementación.

Para un mejor entendimiento de las medidas éstas van a ser explicadas y además van a ser definidos los mecanismos que proporcione el sistema atendiendo a los criterios de categorización. Así se irá delimitando cada una de las medidas y estableciendo en base a los niveles que mecanismos se deberán habilitar para su cumplimiento. Habida cuenta de esta información a continuación se detallarán las diferentes plantillas de seguridad aplicables en función de las diferentes categorías de seguridad.

1.1. MARCO OPERACIONAL

1.1.1. CONTROL DE ACCESO

El control de acceso cubre todo el conjunto de acciones que bien preparatorias o ejecutivas orientadas a determinar qué o quién puede o no acceder a un recurso del sistema, mediante una determinada acción. Con el cumplimiento de todas las medidas se garantizará que nadie accederá a recursos sin la debida autorización. Adicionalmente se establece la necesidad de que el uso del sistema quede registrado para detectar y reaccionar ante una incidencia de seguridad o fallo del sistema.

Toda medida de control de acceso busca el equilibrio entre la usabilidad y la protección del sistema, de tal forma que la seguridad se irá incrementando en base a la categoría exigida. Por lo tanto, se requiere una menor exigencia de seguridad para la categoría básica mientras que en la categoría media y alta se requiere una mayor exigencia.

1.1.1.1. OP. ACC. 1. IDENTIFICACIÓN

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

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

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

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

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

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

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

1.1.1.2. OP. ACC. 4. PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

Este proceso requiere consolidación de los derechos de acceso, de tal forma que:

a) Exista la aplicación del mínimo privilegio. Los privilegios de cada recurso se reducirán al mínimo estrictamente necesario para poder cumplir las obligaciones.

b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.

c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su propietario.

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

En la navegación a Internet o acceso a una aplicación web, un usuario no requiere del privilegio de administrador para desempeñar dichas tareas, ya que de este modo y sin darse cuenta, podría estar poniendo en grave riesgo la seguridad del sistema al tratar ficheros, ejecutables, componentes y otros, descargados de Internet o de otras fuentes de dudosa confianza, con máximos privilegios. Se deberá por lo tanto establecer que, para el acceso a la información sustentada por un sitio web, no requerir privilegios administrativos para acceder a los datos existentes a través del proceso de navegación.

Se deberán establecer así mismo, niveles de control de acceso para impedir que un usuario no autorizado pueda visualizar contenido que no es requerido para las funciones que desempeña. Se establece por lo tanto a nivel de las aplicaciones Web el aplicar mecanismos de ACL para permitir la visualización de contenido a los usuarios que los requieran exclusivamente.

Se deberá tener en consideración debido a dicha norma que los permisos otorgados a los usuarios serán los mínimos requeridos no siendo necesario que estos posean permisos adicionales para la tarea que van a realizar. Por ejemplo, si un desarrollador tiene permiso para acceder a las carpetas donde se aloja el contenido de un sitio web para modificar su código, no por ello implica que sea necesario que posea el permiso de "Control total". Con la concesión de este permiso se le estarían otorgando permisos más allá de las necesidades que requiere dicho usuario. Concederle el permiso de modificar se debe considerar como la opción más óptima desde el punto de vista del ENS.

1.1.1.3. OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN

Dentro de los procesos habituales en el manejo de los sistemas de la información, el relativo a la autenticación en un servidor web antes de acceder a datos, es necesario indicar al sistema "quién eres" usando los métodos de autenticación existentes.

El sistema de autenticación se puede traducir tecnológicamente mediante múltiples mecanismos, siendo el del empleo de una contraseña el más habitual pero no por ello el más seguro, sino todo lo contrario. Los mecanismos de autenticación se deberán adecuar en función del nivel de criticidad de la información o el servicio web atendiendo lógicamente a diferentes criterios.

Según establece el propio Esquema Nacional de Seguridad, a grandes rasgos estos criterios serán los siguientes:

a) Para la categoría básica se admitirá el uso de cualquier mecanismo de autenticación: claves concertadas, dispositivos físicos (en inglés "Tokens"), sistemas de biometría o certificados digitales entre otros.

b) Para la categoría media se desaconseja el empleo de password o claves concertadas, siendo recomendable el uso de sistemas físicos (Tokens), biométricos o certificados digitales.

c) Para la categoría alta, se prohíbe el uso de autenticadores basados en el empleo de claves concertadas. Se exige para ello el uso de dispositivos físicos o biometría. Para ello deberán emplearse algoritmos acreditados por el Centro Criptológico Nacional, recogidos en la guía CCN-STIC-808 de criptología de empleo en el ENS.

Debe tomarse en consideración que Internet Information Services 10 contempla diferentes mecanismos de autenticación incluyendo los de biometría o el uso de certificados emitidos por entidades certificadoras para autenticar. El paso a paso mostrará cómo hacer uso de certificados para la autenticación de clientes de forma general. Si deberá tener en cuenta que cada sitio web dependiendo de la criticidad de la información deberá ajustarse a requisitos específicos para operar con certificados de autenticación o sistemas de biometría.

1.1.1.4. OP. ACC. 7. ACCESO REMOTO

La organización deberá mantener las consideraciones de seguridad, en cuanto al acceso remoto, cuando éstas se realicen fuera de las propias instalaciones de la organización y a través de redes de terceros.

Éstas deberán también garantizar la seguridad, tanto en el propio acceso en sí, como en el canal del acceso remoto.

IIS 10 faculta el empleo de protocolos seguros para las comunicaciones y los procesos de autenticación usando HTTPS que utiliza un cifrado basado en SSL/TLS para crear un canal cifrado para el tráfico de información sensible.

Para que el servidor web acepte las conexiones HTTPS se debe haber creado previamente un certificado de clave pública, dicho certificado debe estar firmado por una autoridad de certificación para que el navegador lo acepte.

1.1.2. EXPLOTACIÓN

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

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

1.1.2.1. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD

Se considera que IIS 10 debe configurarse previamente a su entrada en producción teniendo en cuenta las siguientes directrices:

a) Se retiren cuentas y contraseñas estándar.

b) Se aplique la regla de mínima funcionalidad.

Para el servidor web se considera indispensable que el sistema no proporcione funcionalidades gratuitas. Solamente las estrictamente necesarias. Esto permitirá adaptarse al principio de mínima exposición. Para ello se eliminarán o desactivarán, mediante el control de la configuración, aquellas funciones que no sean necesarias e incluso aquellas que sean inadecuadas al fin que se persigue.

Para el cumplimiento en este sentido, las diferentes plantillas de seguridad se dotarán de las funcionalidades necesarias para deshabilitar y configurar todos aquellos servicios que, no siendo necesarios para ningún entorno operativo, pudieran constituir un riesgo de seguridad. Adicionalmente, se protegerán los más importantes de tal forma que quedarán configurados, a través de las políticas de grupo que correspondieran, por categorías. Se facilitarán consejos para conocer y gestionar los servicios implicados y cómo actuar ante riesgos de seguridad identificados en la red.

Adicionalmente se deshabilitarán, como parte de los mecanismos de mínima funcionalidad y mínima exposición de la información manejada. Debe valorarse la información remitida al fabricante en función de los acuerdos de soporte establecidos con el mismo y/o las normativas de seguridad internas referidas a la transmisión de datos a Internet.

1.1.2.2. OP. EXP. 3. GESTIÓN DE LA CONFIGURACIÓN

Se deberá tener en consideración la configuración de los componentes del sistema que se gestione de forma que:

a) Se mantenga en todo momento la regla de funcionalidad mínima y seguridad por defecto.

b) El sistema debe adaptarse a las nuevas necesidades las cuales previamente han sido autorizadas y probadas en un entorno de test antes de la puesta en producción.

c) El sistema debe reaccionar ante vulnerabilidades reportadas e incidentes.

1.1.2.3. OP. EXP. 5. GESTIÓN DE CAMBIOS

Para las categorías media y alta de seguridad se mantendrá un control continuo de los cambios realizados en el sistema, por lo que, todos los cambios anunciados por el proveedor o fabricante deberán serán analizados previamente para establecer su conveniencia en la incorporación al sistema o no.

Previamente a la puesta en producción de una modificación, se ha de comprobar su correcta funcionalidad en el sistema en un entorno que no esté en producción, este entorno debe ser un fiel reflejo del entorno de producción.

Todos los cambios realizados deben ser planificados con anterioridad para minimizar en la medida de lo posible el impacto sobre la prestación de los servicios afectados.

Se ha de tener en consideración mediante un análisis de riesgos si los cambios a realizar son de mayor o menor relevancia para la seguridad del sistema, por ello, aquellos cambios que impliquen una situación de riesgo de nivel alto deberán ser aprobados explícitamente de forma previa a su implantación.

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

Aplicable en las categorías altas de seguridad, se deberán implementar mecanismos para garantizar la trazabilidad de las acciones de los usuarios. Para ellos se deberá conocer:

IIS 10 implementa mecanismos para la auditoría de los sistemas e infraestructuras. El problema consiste en que, de forma predeterminada, los datos son almacenados localmente. Existen, no obstante, mecanismos nativos para la suscripción y recolección de eventos. La guía CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2 permitirá establecer los procedimientos para la recogida y análisis de los registros de auditoria, desde múltiples sistemas, permitiendo establecer mecanismos de correlación.

En IIS 10 se registrará la actividad de los usuarios para indicar quien realiza la actividad, cuando la realiza y sobre qué información para poder detectar y reaccionar a cualquier fallo accidental o deliberado.

También se contempla el registro de la actividad de los usuarios y en especial de los operadores y administradores en cuanto al acceso a la configuración y mantenimiento del servidor web.

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

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

Adicionalmente el Servidor de ficheros dispone de mecanismo que permiten emitir informes sobre todo aquello que se almacena, modifica o elimina en él pudiendo realizar seguimientos y acciones correspondientes.

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

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

a) Determinar el período de retención de los registros.

b) Asegurar fecha y hora del registro de la actividad

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

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

Nuevamente, en la guía CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2, se articulan los mecanismos para garantizar la disponibilidad y retención de los registros, así como los procedimientos operativos para su salvaguarda.

1.2. MEDIDAS DE PROTECCIÓN

1.2.1. PROTECCIÓN DE LAS COMUNICACIONES

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

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

El Real Decreto 3/2010 de 8 de enero, de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

1.2.1.1. MP. COM. 3. PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD

Se deberá asegurar la autenticidad del otro extremo en un canal de comunicaciones antes de proceder al intercambio de datos entre los mismos. Además, deberán prevenirse ataques activos, garantizando que los mismos serán detectados, permitiendo activarse los procedimientos previstos en el tratamiento frente a incidentes usando los mecanismos de autenticación establecidos anteriormente expuestos en este documento en el punto "1.1.1.3 OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN".

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

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

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

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

En el caso de ser necesario asegurar la confidencialidad de las comunicaciones Web, es necesario hacer uso de la versión segura del protocolo, HTTPS. HTTPS utiliza SSL (Secure Socket Layer) o TLS (Transport Layer Security) para cifrar las comunicaciones entre el navegador Web y el servidor Web.

La gestión de sesiones en la aplicación Web debe realizarse empleando identificadores de sesión o tokens no predecibles, de suficiente longitud para que no puedan ser resueltos mediante técnicas de fuerza bruta, y que caduquen tras cierto tiempo.

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

Desde el punto de vista de la infraestructura Web, se debe disponer de un análisis detallado del usuario, grupo, permisos y derechos con los que ejecutarán cada uno de los componentes de la aplicación Web como, por ejemplo, los procesos del servidor Web o de aplicación. Este análisis permitirá aplicar todos los mecanismos de autorización necesarios.

Las cabeceras HTTP pueden ser manipuladas fácilmente por un atacante y no deben emplearse como método de validación o de envío de información. 60. Todos los mecanismos de interacción entre los distintos componentes del entorno Web (servidor Web, de aplicación y base de datos) deben realizarse de forma segura. Las comunicaciones entre estos elementos deberán estar cifradas, autentificadas y asegurarse su integridad.

Adicionalmente a los elementos de seguridad propios de un entorno Web, es necesario proteger todos los elementos de la infraestructura en la que reside la aplicación Web, tales como dispositivos de comunicaciones (routers, switches, etc) o la infraestructura de servidores de nombres (DNS).

1.2.1.2. MP. INFO. 6. LIMPIEZA DE DOCUMENTOS

El proceso de limpieza de documentos afecta a las tres categorías de seguridad por igual y se ha de tener en consideración que se retiraran todos los datos de los documentos además de la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, con la excepción de la información pertinente para el receptor del documento.

El incumplimiento de esta medida puede perjudicar especialmente:

a) Al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento.

b) Al mantenimiento de la confidencialidad de las fuentes u orígenes de la información, que no debe conocer el receptor del documento.

c) A la buena imagen de la organización que difunde el documento por cuanto demuestra un descuido en su buen hacer.

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

Todos los sistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que le competen como:

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

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

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

Uno de los elementos principales empleados en la protección de entornos de aplicaciones Web son los cortafuegos (firewalls) de aplicaciones Web, también conocidos como WAF, Web Application Firewall.

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

Algunos ataques Web, como por ejemplo XSS o inyección SQL, pueden ser mitigados filtrando los datos maliciosos (código HTML y scripts, o sentencias SQL, respectivamente) en la entrada de la aplicación, en la salida, o en ambas. Se recomienda, aplicando criterios de defensa en profundidad, aplicar los mecanismos de filtrado tanto en la entrada como en la salida.

Para las diferentes categorías de seguridad se emplearán certificados cualificados de autenticación del sitio web acorde a la normativa europea.

2. RESUMEN Y APLICACIÓN DE MEDIDAS DE IIS 10 SOBRE WINDOWS SERVER 2016

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

Control	Medida	Mecanismo de aplicación
OP. ACC. 1	Segregación de roles y tareas	Revisión e implementación de guía CCN-STIC-574, adaptándolos a la organización.
OP. ACC. 4	Gestión de derechos de acceso	Revisión e implementación de guía CCN-STIC-574, adaptándolos a la organización.
OP. ACC. 5	Mecanismos de autenticación	Revisión e implementación de guía CCN-STIC-574, adaptándolos a la organización.
OP. ACC. 7	Protocolos de autenticación en red	Revisión e implementación de guía CCN-STIC-574, adaptándolos a la organización.
OP. EXP. 2	Control de funcionalidad de servicios para garantizar el principio de mínima funcionalidad	Revisión e implementación de guía CCN-STIC-574, adaptándolos a la organización.
OP. EXP. 3	Gestión de la configuración	Revisión e implementación de guía CCN-STIC-574, adaptándolos a la organización.
OP. EXP. 8	Registro de actividad de los usuarios	Revisión e implementación de guía CCN-STIC-572, adaptándolos a la organización. Se debe tomar en consideración que el RD 951/2015 cambia la medida con respecto a lo establecido en RD 3/2010. En la actualidad el requisito del registro de actividad es requerido desde la categoría básica. Revisión e implementación guía CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2.
OP. EXP. 9	Registro de la gestión de incidentes	Revisión e implementación de guía CCN-STIC-574, adaptándolos a la organización.
OP. EXP. 10	Protección de los registros de actividad	Revisión e implementación de guía CCN-STIC-574, adaptándolos a la organización.
MP. COM. 3	Protección de la autenticación y de la integridad	Revisión e implementación de guía CCN-STIC-574, adaptándolos a la organización.

ANEXO A.2. CATEGORÍA BÁSICA

ANEXO A.2.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 MIEMBROS DEL DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

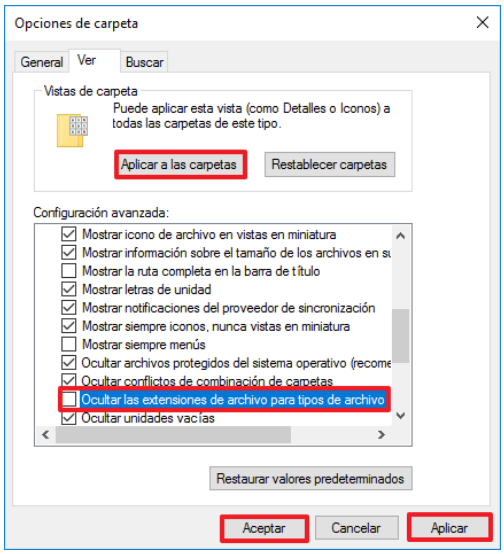
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tenga que securizar IIS 10 sobre Microsoft Windows Server 2016 con una categorización de seguridad básica según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría básica, deberá realizar las implementaciones según se referencian en el presente anexo.

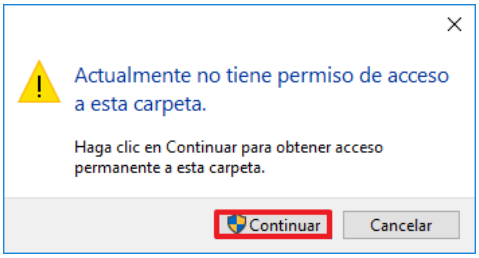
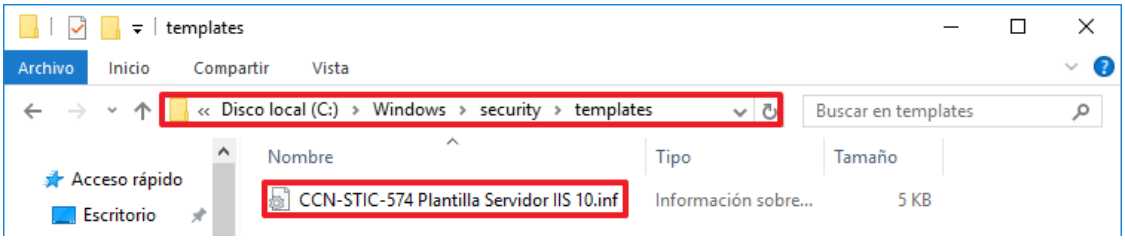
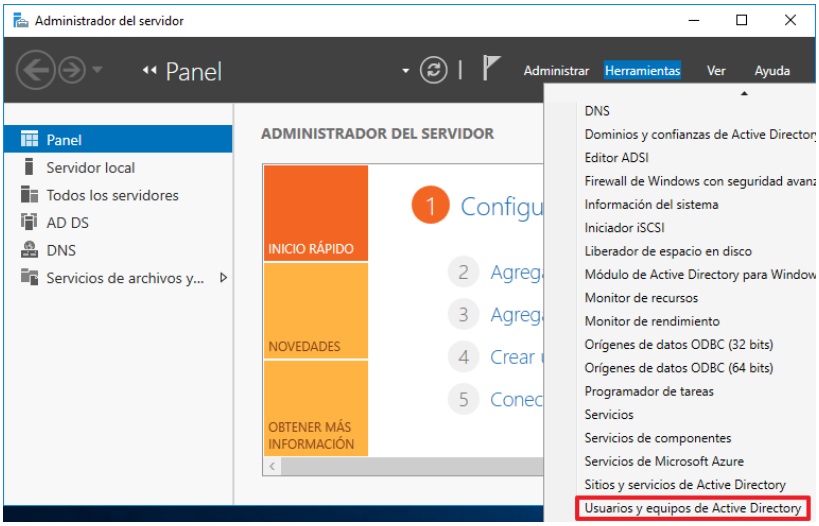
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

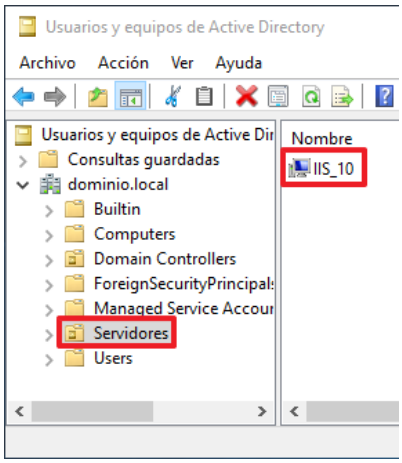
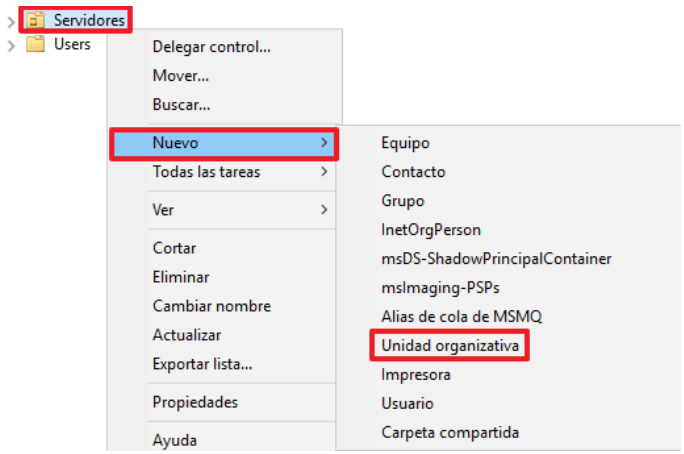
1. PREPARACIÓN DEL DOMINIO

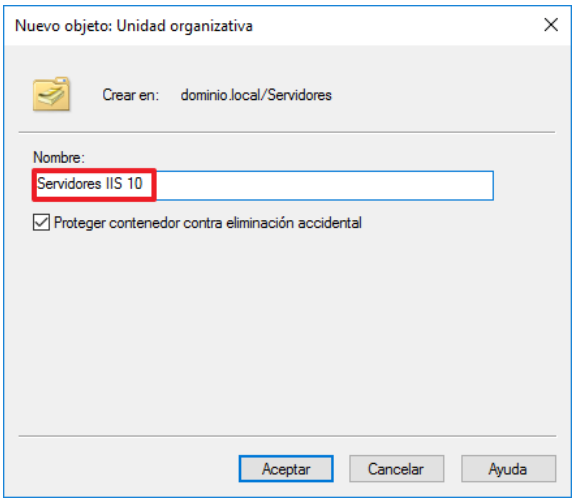
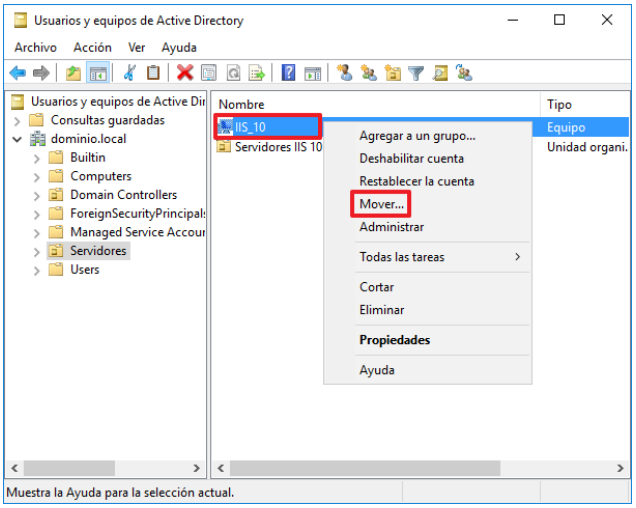
Los pasos que se describen a continuación se realizarán en un controlador de dominio del domino al que va a pertenecer el servidor Internet Information Services 10.

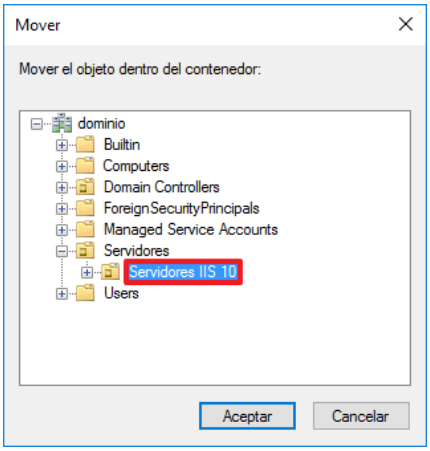
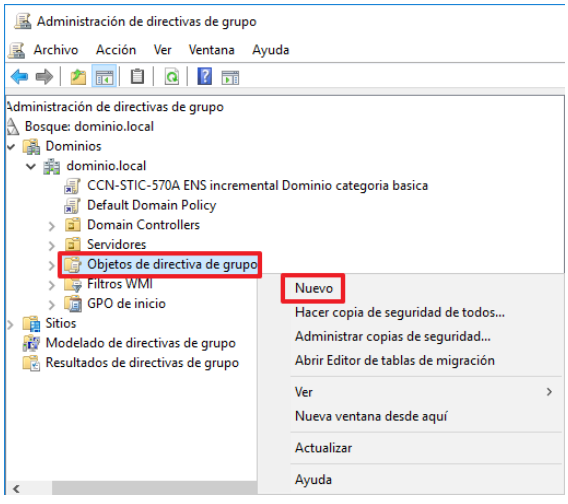
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.

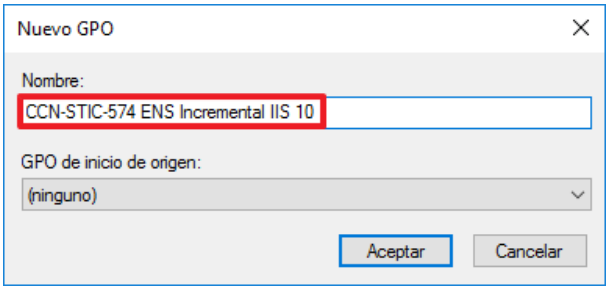
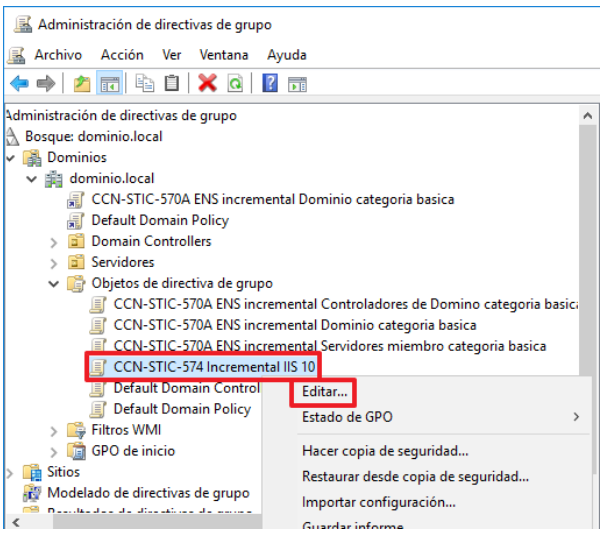
Paso	Descripción
4.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar “Explorador de Windows” y poder mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”, se despliega la opción “Cambiar opciones de carpeta y búsqueda”. De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura:  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

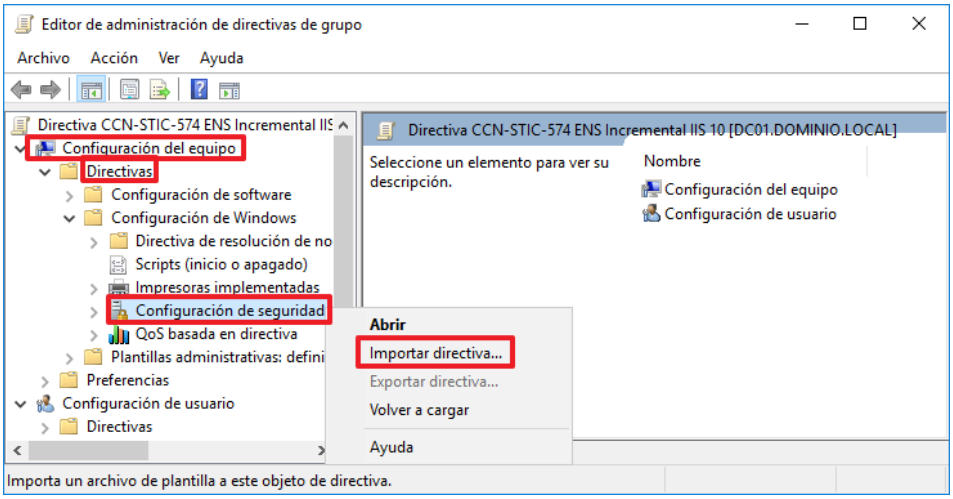
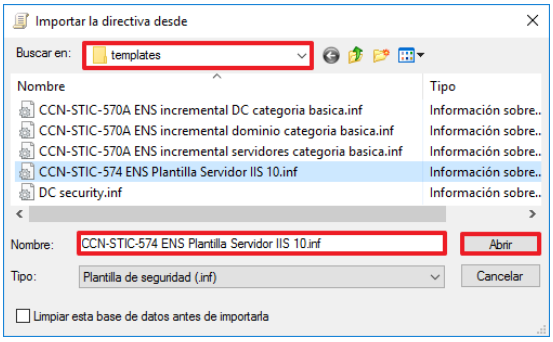
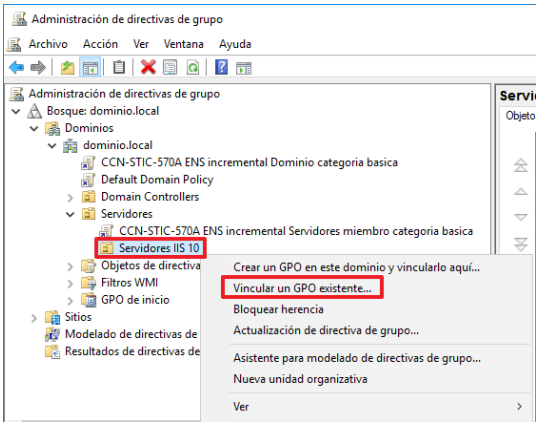
Paso	Descripción
5.	Copie el fichero “CCN-STIC-574 ENS Plantilla Servidor IIS 10.inf” al directorio “%SYSTEMROOT%\Security\Templates” del controlador de dominio.   **Nota:** Según la configuración de seguridad de UAC, el sistema podría solicitar la elevación de privilegios por cada uno de ellos, en este caso, pulse “Continuar” en las 3 ocasiones que el sistema se lo solicita o marque la opción “Hacer esto para todos los elementos actuales” para pulsar “Continuar” en una sola ocasión.
6.	Inicie la herramienta de usuarios y equipos del Directorio Activo. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor”. “**Herramientas → Usuarios y equipos de Active Directory”**. 

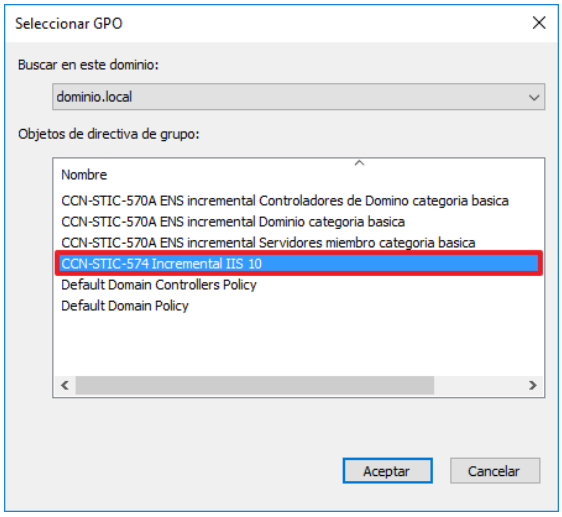
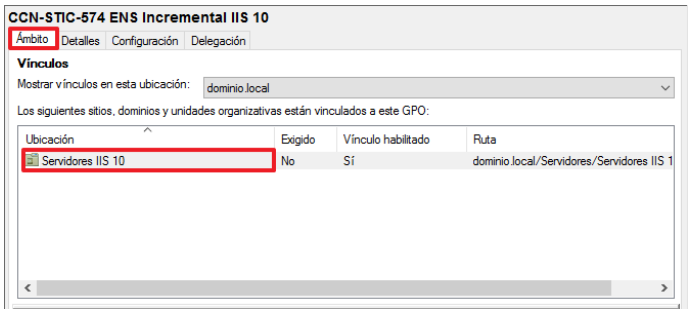
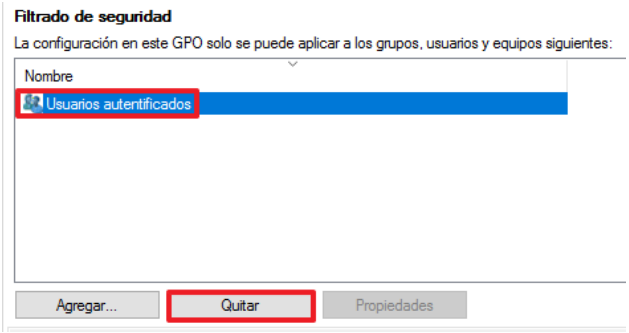
Paso	Descripción
7.	Despliegue el dominio y vaya a la carpeta “Servidores”. **“Menú inicio → Herramientas administrativas → Usuarios y equipos de Active Directory → [nombre del dominio] → Servidores”**.  **Nota:** Si usted no desea crear unidades organizativas en su organización deberá adaptar estos pasos para alojar los servidores IIS 10 y vincular la GPO que se creará posteriormente a los servidores IIS 10 de su organización.
8.	Solicite la creación de una nueva unidad organizativa utilizando el menú contextual, pulse botón derecho sobre la unidad organizativa “Servidores” y despliegue **“Nuevo → Unidad organizativa”**. 

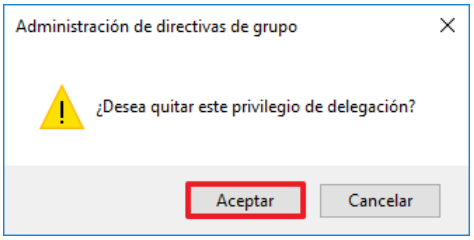
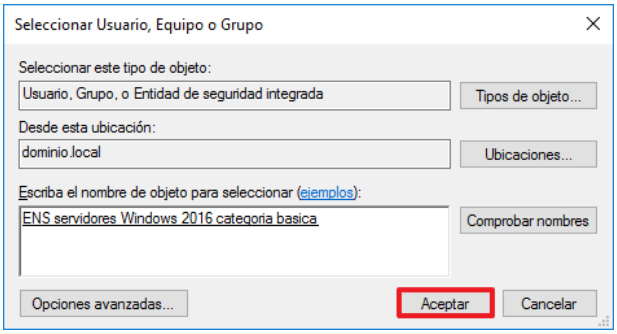
Paso	Descripción
9.	En la consola, cree una unidad organizativa denominada “Servidores IIS 10” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen. 
10.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores IIS 10 a la unidad organizativa “Servidores IIS 10”. Para ello, deberá hacer clic botón derecho sobre “mover” en el servidor que desee ubicar en la nueva unidad organizativa. 

Paso	Descripción
11.	A continuación, seleccionamos la unidad organizativa “Servidores IIS 10”. 
12.	Cierre la herramienta de “Usuarios y equipos de Directorio Activo”
13.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor”. **“Herramientas → Administración de directivas de grupo”**. 
14.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”.
15.	Pulse con el botón derecho, sobre dicha carpeta y seleccione la opción “Nuevo”. 

Paso	Descripción
16.	Introduzca como nombre “CCN-STIC-574 ENS Incremental IIS 10” y pulse el botón “Aceptar”. 
17.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
18.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**

Paso	Descripción
19.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva…”. 
20.	Seleccione de la ruta “C:\Windows\security\templates” el fichero “CCN-STIC-574 ENS Plantilla Servidor IIS 10.inf” y pulse el botón “Abrir”. 
21.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
22.	A continuación, seleccione la unidad organizativa “Servidores IIS 10” y pulse botón derecho, “Vincular un GPO existente…”. 

Paso	Descripción
23.	Seleccione el objeto de directiva de grupo con nombre, “CCN-STIC-574 ENS Incremental IIS 10” y pulse aceptar. 
24.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
25.	Seleccione la nueva política de grupo configurada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 
26.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 

Paso	Descripción
27.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
28.	Una vez quitado, pulse el botón “Agregar…”.
29.	Introduzca como nombre “ENS servidores Windows 2016”. Este grupo corresponde con el generado en la aplicación de la guía CCN-STIC-570A. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

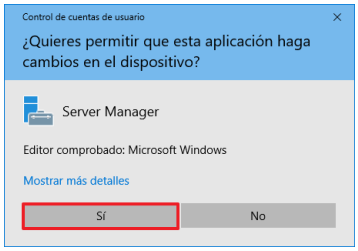
El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto,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

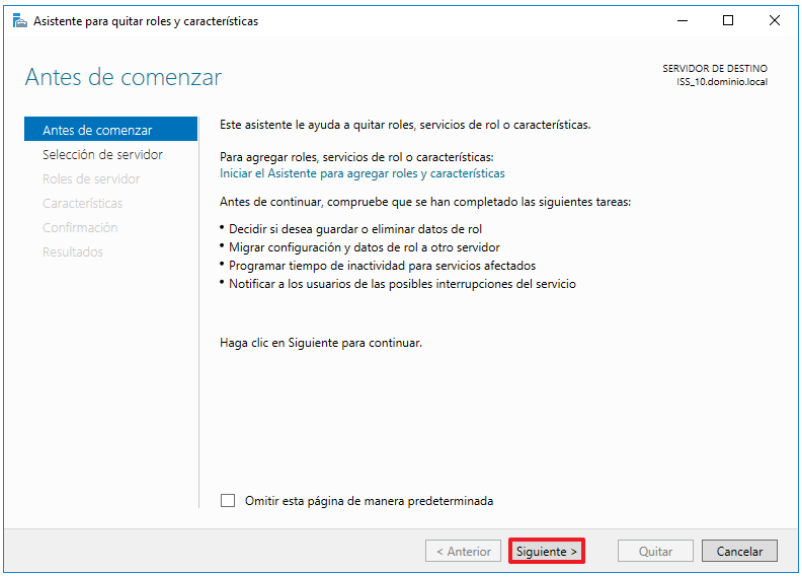
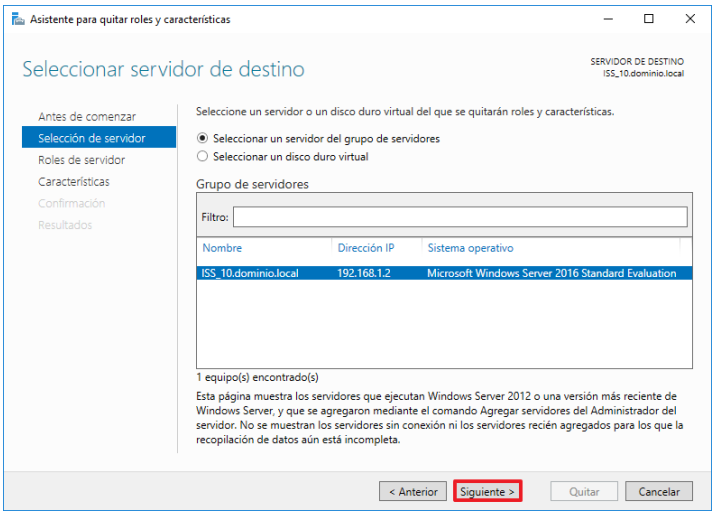
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

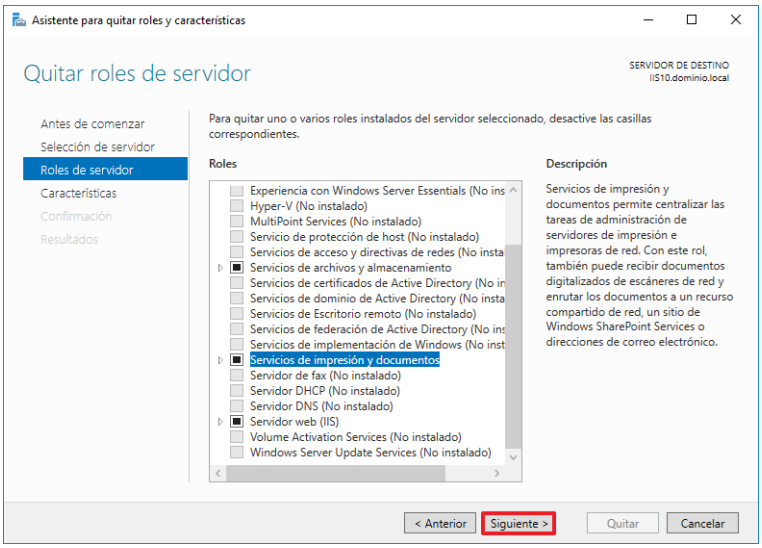
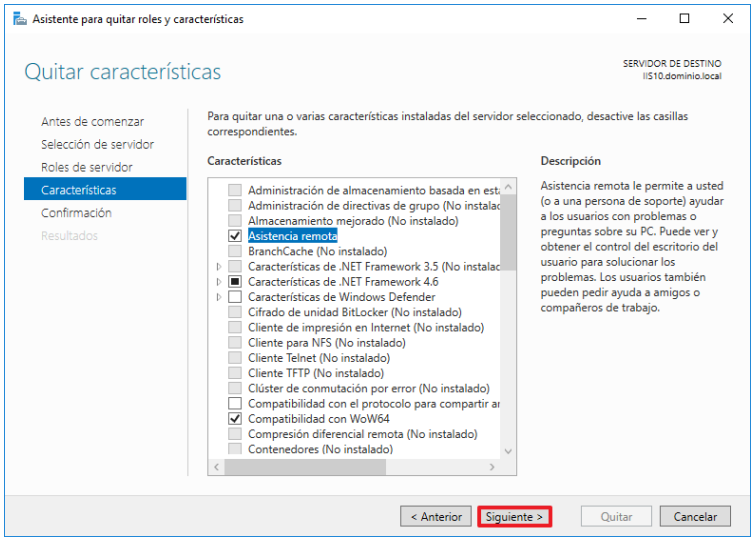
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

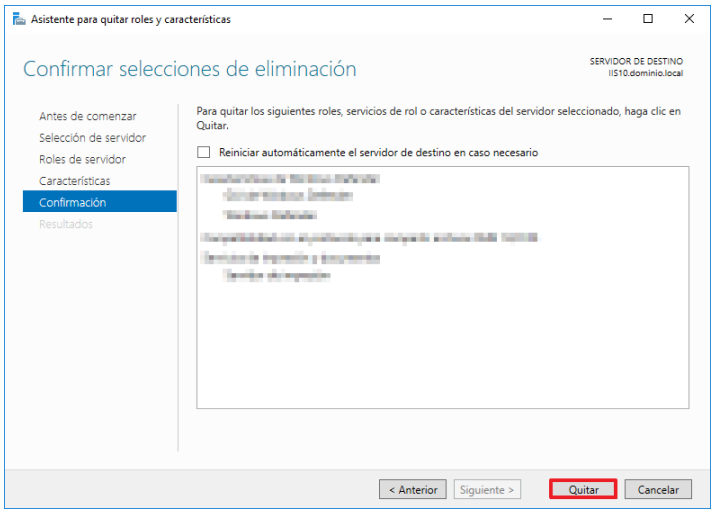
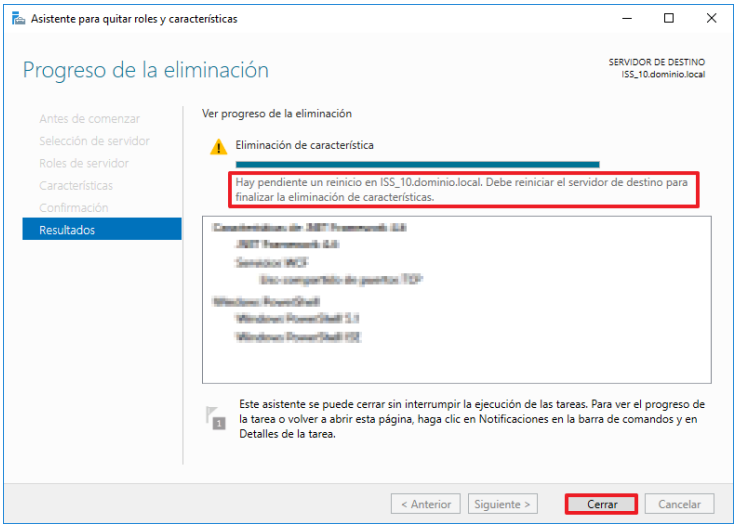
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

Es recomendable que el sitio web este alojado en otra ubicación de disco diferente a la del sistema operativo y que esta solo se utilice para el alojamiento de sitios web, evitando con ello exponer más información de la estrictamente necesaria.

Paso	Descripción
30.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado el rol de IIS 10. 
31.	Pulse sobre el administrador del servidor. 
32.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 

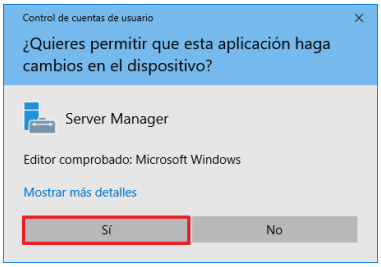
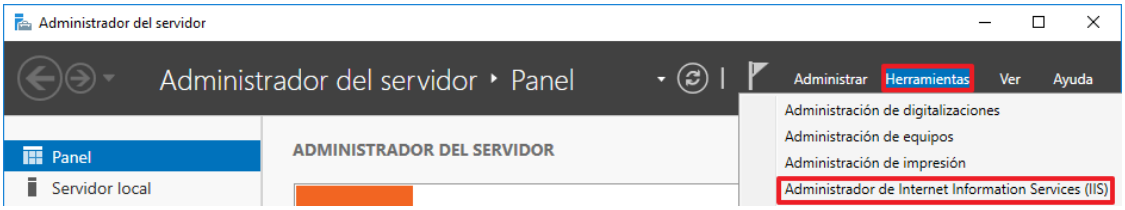
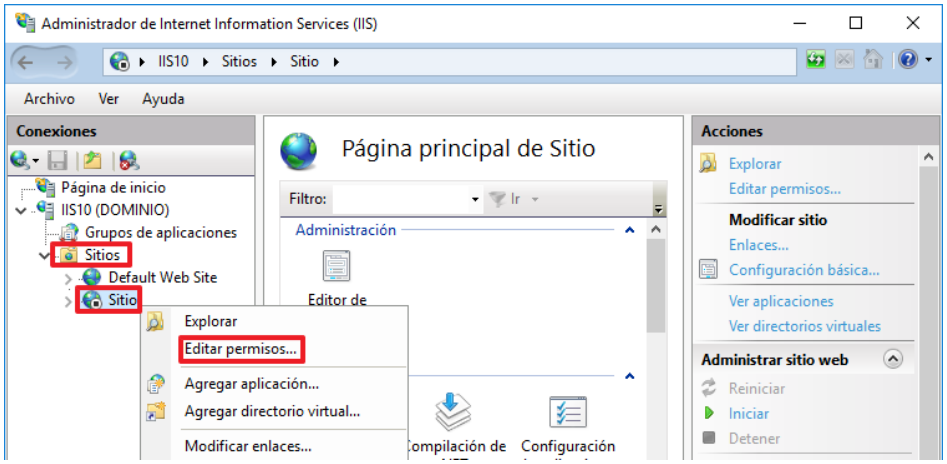
Paso	Descripción
33.	A continuación, pulse sobre el menú superior de la derecha de la herramienta "Administrador del servidor". **"Administrar → Quitar roles y funciones"**. 
34.	Comenzará el asistente para quitar roles y características, pulse sobre el botón **"Siguiente >"**. 
35.	Seleccione el servidor donde desea quitar las características del IIS 10 y pulse siguiente. 

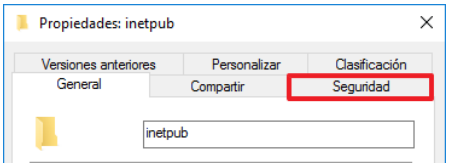
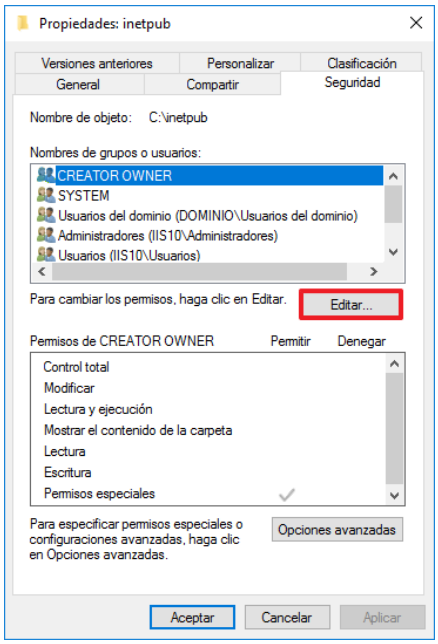
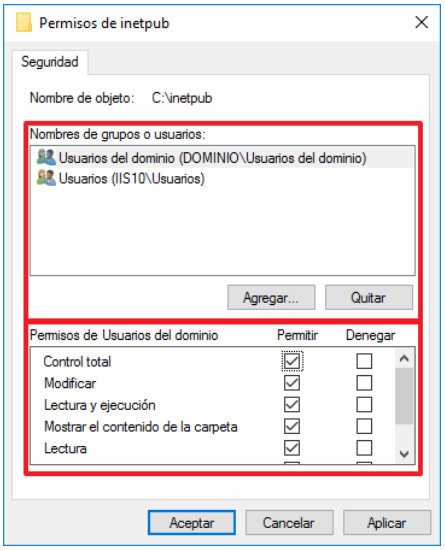
Paso	Descripción
36.	En la siguiente ventana podrá quitar roles del servidor, en este caso pulse siguiente para acceder a las características de los roles instalados. 
37.	A continuación, seleccione las características que desea quitar. 

Paso	Descripción
38.	La siguiente pantalla mostrara las características a modos resumen que desea quitar, confirme que las características seleccionadas son las correctas y pulse “Quitar”. 
39.	Una vez finalizada la desinstalación pulse “Cerrar”.  **Nota:** Debe tener en cuenta que la desinstalación de determinadas características puede requerir el reinicio del equipo.

2.2. GESTIÓN DE PERMISOS RECURSOS WEB

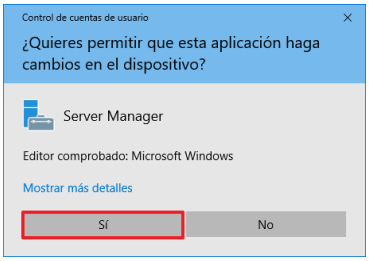
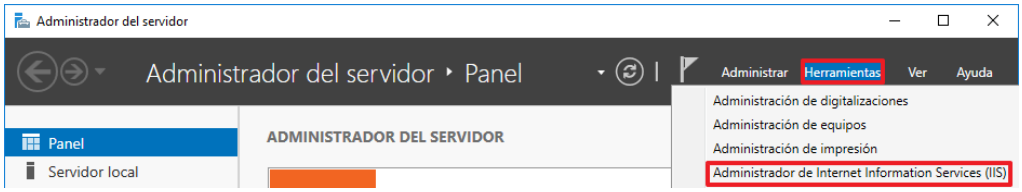
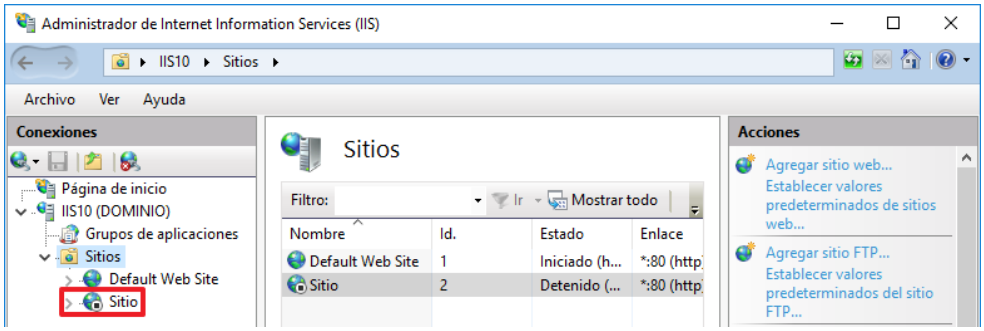
En este apartado se tendrá en consideración la gestión y administración del acceso a los recursos web según el marco operacional de categoría básica establecido por el ENS, para con ello limitar y controlar el acceso a directorios con información sensible de ser sustraída.

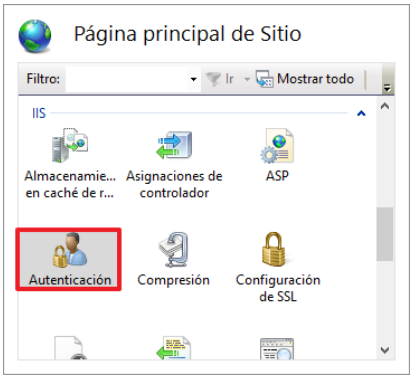
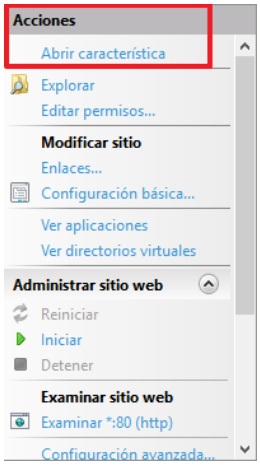
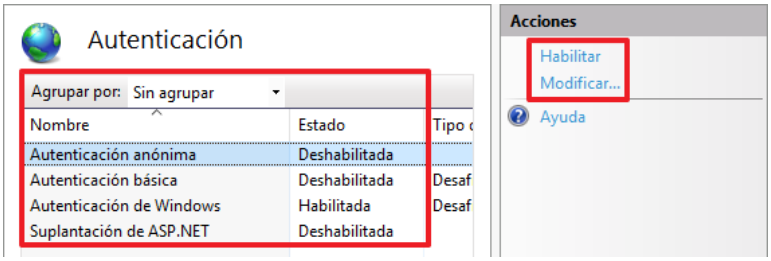
Paso	Descripción
40.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
41.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 
42.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor”. **“Herramientas → Administrador de Internet Information Services (IIS)”**. 
43.	Pulse botón derecho sobre el sitio al cual quiere asignar o quitar permisos. 

Paso	Descripción
44.	Diríjase hasta la pestaña seguridad. 
45.	A continuación, pulse el botón “Editar”. 
46.	A continuación, seleccione los permisos del que desea establecer para ese sitio web.  **Nota:** Es recomendable dar permiso solo a los usuarios o grupos que deban tener acceso al sitio web evitando que el usuario administrador tenga permiso para prevenir posibles vulnerabilidades.

2.3. AUTENTICACIÓN SITIO WEB

Los métodos de autenticación permitirán limitar el acceso al sitio web a una lista determinada de usuarios (el método habilitado por defecto de los servicios web de IIS es la autenticación anónima), en todas las categorías de seguridad se debe limitar el acceso al contenido web a usuarios anónimos para prevenir posibles ataques.

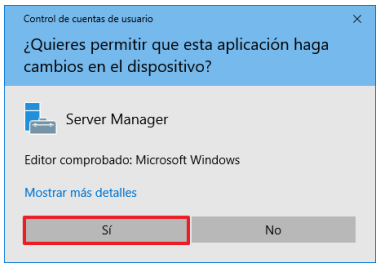
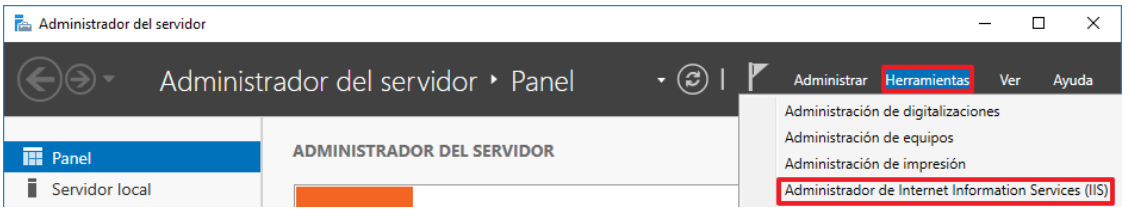
Paso	Descripción
47.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
48.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar. 
49.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor”. **“Herramientas → Administrador de Internet Information Services (IIS)”.** 
50.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo de “Conexiones” y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.

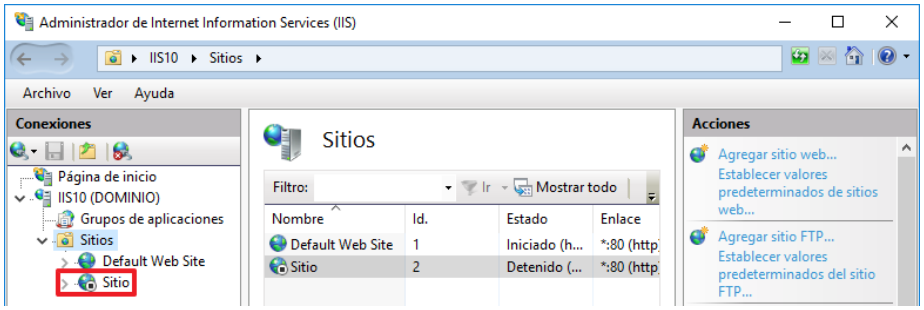
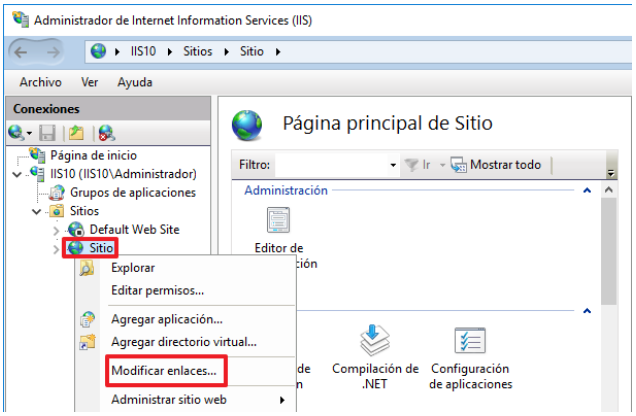
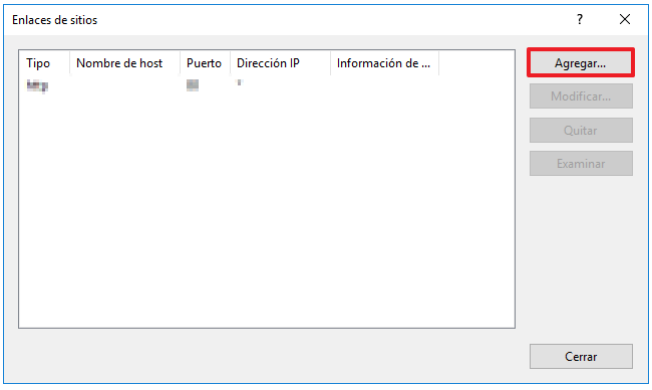
Paso	Descripción
51.	Seleccione en la página principal del sitio web el icono de “Autenticación”. 
52.	Pulse sobre “Abrir característica” situado en el panel derecho en el menú “Acciones”. 
53.	A continuación, establezca según las características de su organización los métodos de autenticación disponibles. Para ello pulse sobre el método de autenticación que quiere configurar y en el panel derecho seleccione la acción que desea realizar.  **Nota:** Únicamente se usará la autenticación anónima para páginas webs generales en la que solo se muestre contenido y no sea necesaria la autenticación del usuario.

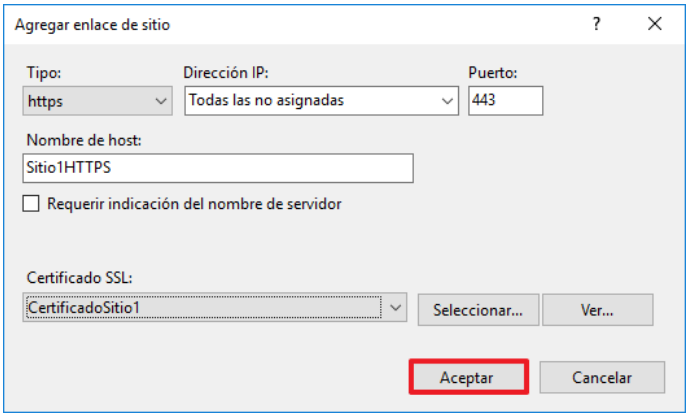
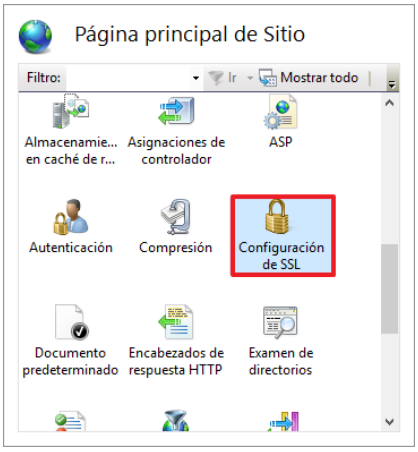
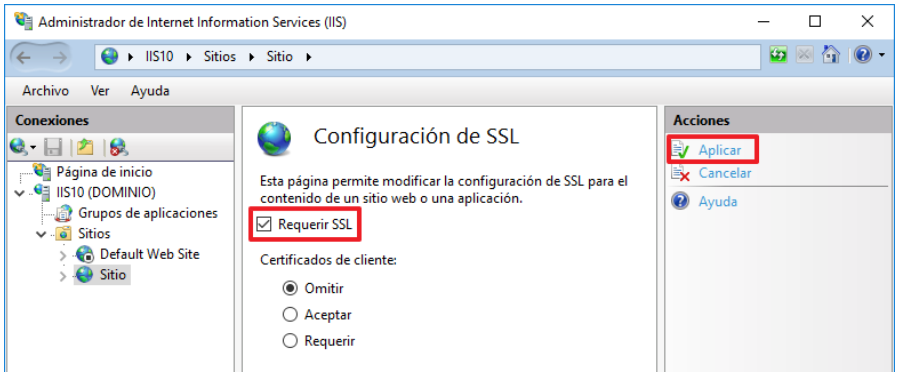
2.4. CERTIFICADOS

IIS 10 faculta el empleo de protocolos seguros para las comunicaciones y los procesos de autenticación usando HTTPS que utiliza un cifrado basado en SSL/TLS para crear un canal cifrado para el tráfico de información sensible,

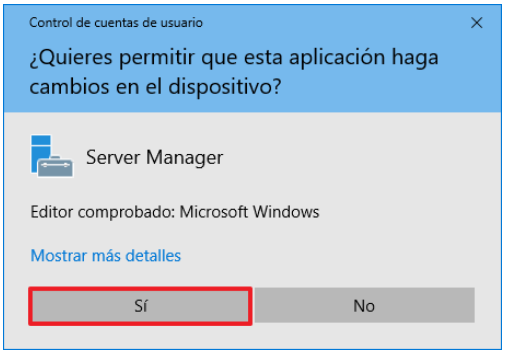
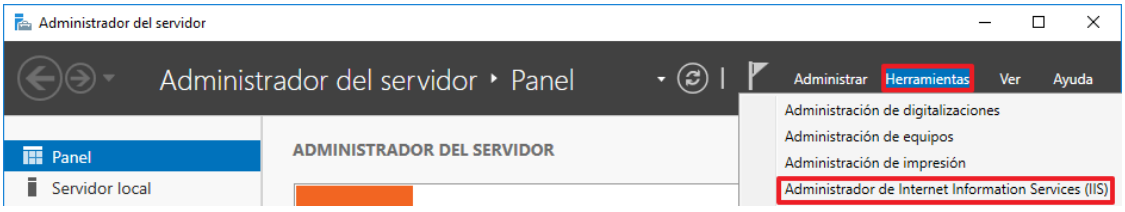
Para sitios públicos es recomendable el uso de certificados emitidos por CA de terceros reconocidas, en el caso de sitios web internos es recomendable el uso de una entidad certificadora interna, desaconsejando el uso de certificados autofirmados.

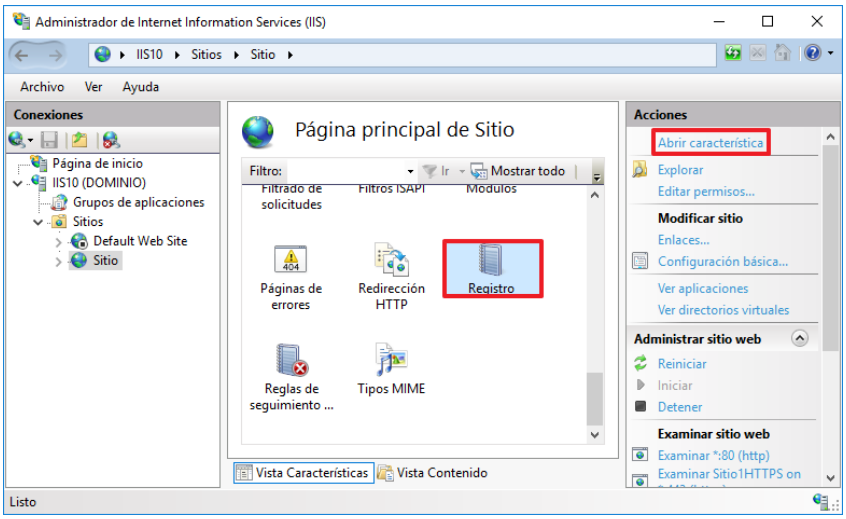
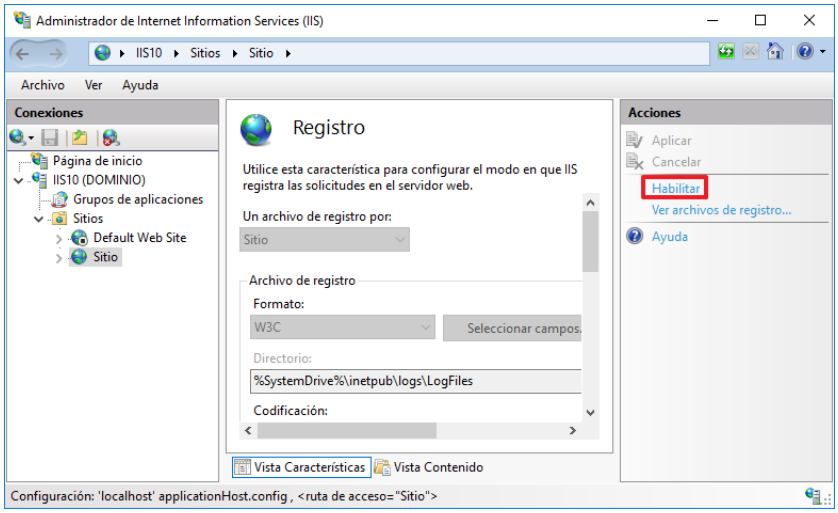
Paso	Descripción
54.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
55.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 
56.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor”. **“Herramientas → Administrador de Internet Information Services (IIS)”.** 

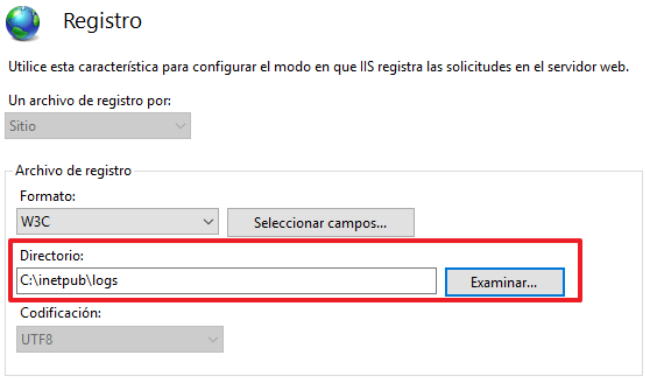
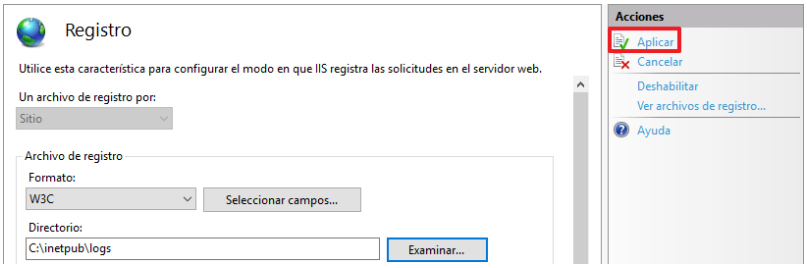
Paso	Descripción
57.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo de “Conexiones” y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.
58.	Pulse con el botón derecho sobre el sitio web que quiere modificar y seleccione la opción “Modificar enlaces…”. 
59.	Pulse sobre el botón “Agregar…”. 

Paso	Descripción
60.	Seleccione Tipo: “https”, seleccione Certificado SSL: “CertificadoSitio1” y pulse sobre “Aceptar”. 
61.	A continuación, deberá configurar el sitio web para que los usuarios requieran un certificado propio, para ello pulse sobre en el sitio web que desea configurar, y seleccione “Configuración de SSL”. 
62.	Seleccione la opción de “Requerir SSL” y pulse sobre “Aplicar” para que el sistema guarde los cambios realizados. 

2.5. AUDITORÍA

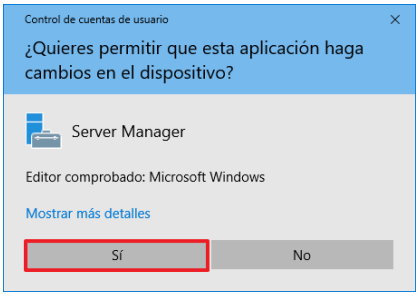
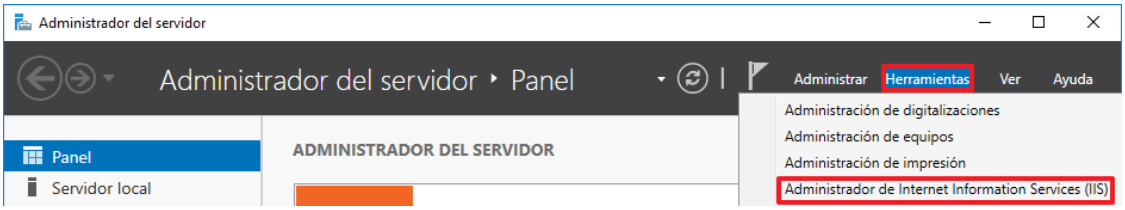
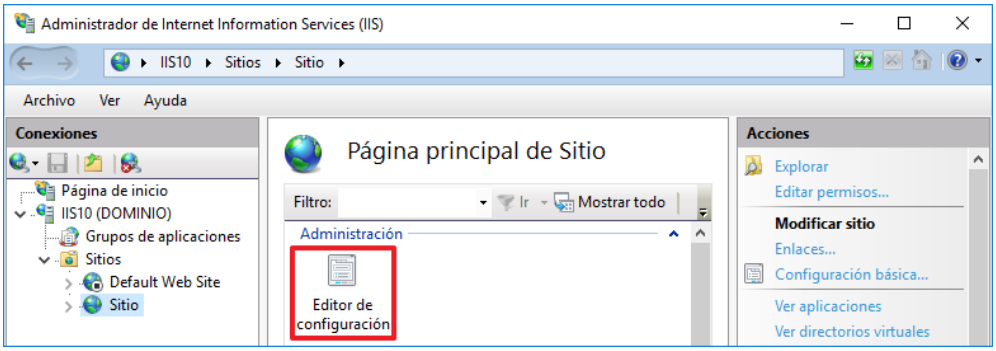
Paso	Descripción
63.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
64.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 
65.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor”. **“Herramientas → Administrador de Internet Information Services (IIS)”** 

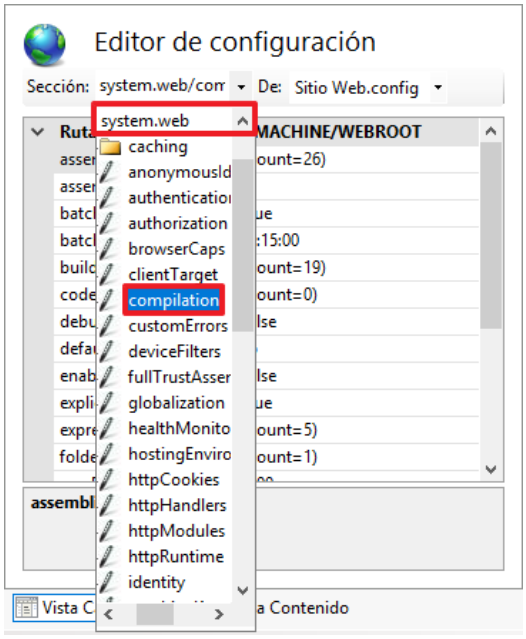
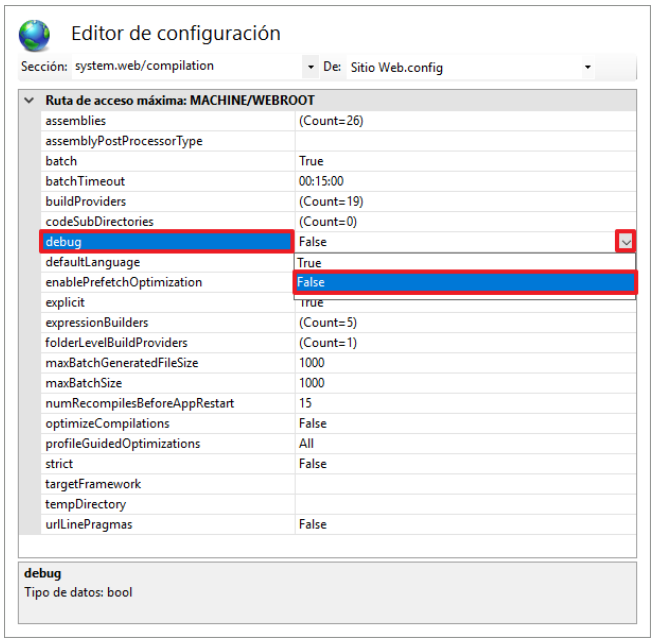
Paso	Descripción
66.	Diríjase al sitio web que desea administrar, a continuación, localice el icono “Registro”, y pulse la acción “Abrir característica” situado en la parte superior derecha de la pantalla para acceder a la configuración del registro. 
67.	Debe habilitar el registro de las solicitudes del servidor IIS 10 para ello, diríjase al menú “Acciones” situado en la parte superior derecha de la pantalla y pulse sobre “Habilitar”. 

Paso	Descripción
68.	A continuación, seleccione el directorio donde se van a guardar los registros, por seguridad es recomendable realizarlo en una unidad diferente a la de la instalación del sistema operativo. 
69.	Una vez realizados los cambios deberá guardarlos, para ello pulse “Aplicar” situado en el menú “Acciones” en la parte superior izquierda de la pantalla. 

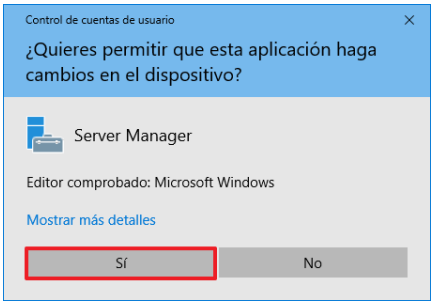
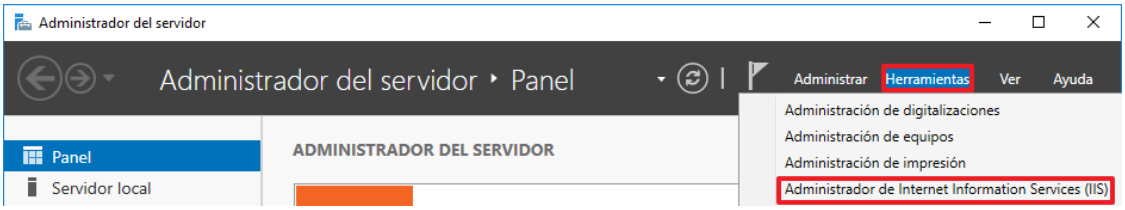
2.6. DESHABILITAR MODOS DE DEPURACIÓN

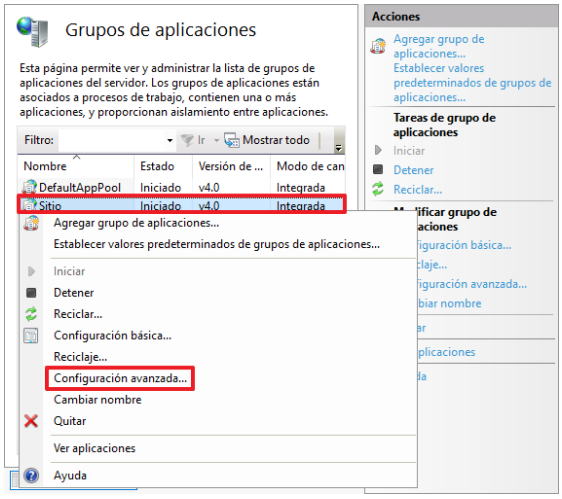
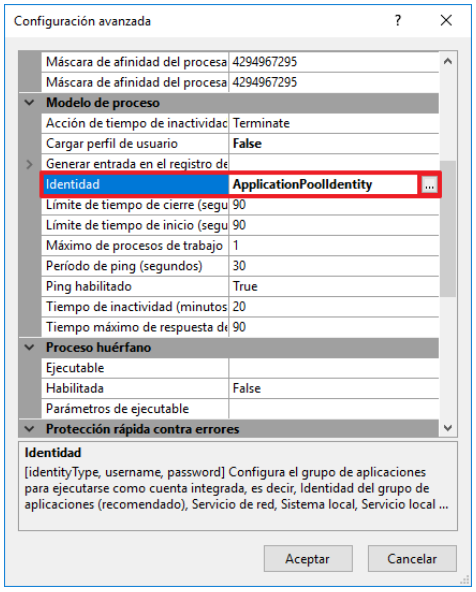
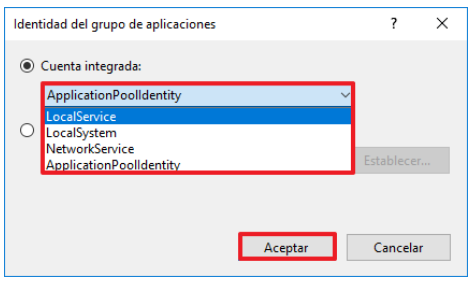
Paso	Descripción
70.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 

Paso	Descripción
71.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 
72.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor”. **“Herramientas → Administrador de Internet Information Services (IIS)”** 
73.	Localice el sitio web que desea configurar y seleccione “Editor de configuración”, a continuación, pulse en el menú “Acciones” la opción “Abrir característica” situado en la parte superior derecha de la pantalla para abrir el editor de configuración. 

Paso	Descripción
74.	Navegue en “Sección” hasta “system.web/compilation”. 
75.	Localice la opción “Debug”, abra el desplegable y seleccione “False”. 

2.7. IDENTIDADES DEL GRUPO DE APLICACIONES

Paso	Descripción
76.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
77.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 
78.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor”. **“Herramientas → Administrador de Internet Information Services (IIS)”** 
79.	Despliegue el servidor y seleccione la opción “Grupos de aplicaciones”. 

Paso	Descripción
80.	A continuación, seleccione la aplicación que desea configurar y haga clic botón derecho sobre ella y pulse “Configuración avanzada…”. 
81.	Localice la opción “Identidad” dentro de “Modelo de proceso”. 
82.	A continuación, seleccione la opción que más se adecue a sus necesidades y pulse “Aceptar”. 

2.8. LIMPIEZA DE METADATOS

Se ha de tener en consideración que en un servidor web se pueden alojar documentos que pueden contener información oculta en los metadatos los cuales contienen información que permite catalogar, ordenar y clasificar archivos, por lo que pueden ser un riesgo de seguridad para la organización, por lo que hay que tener especial atención en la limpieza de los metadatos de los documentos que se alojan en el servidor web por ello antes de alojar un fichero en el servidor web se ha debido de realizar el procedimiento indicado en MP. INFO. 6. LIMPIEZA DE DOCUMENTOS.

En el proceso de limpieza se ha de tener en consideración que se retiraran todos los datos de los documentos además de la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, con la excepción de la información pertinente para el receptor del documento.

2.9. SOLUCIONES WAF (WEB APLICATION FIREWALL)

Un servidor web puede alojar aplicaciones por lo que es importante un control exhaustivo de estas por ello se han de emplear uno de los elementos principales en la protección de entornos de aplicaciones Web que son los cortafuegos (firewalls) de aplicaciones Web, también conocidos como WAF, Web Application Firewall.

El WAF se encargará de proteger los servidores de aplicaciones web de determinados ataques específicos en Internet además de controlar las transacciones al servidor web de nuestra organización.

Este sistema nos permite evitar probables ataques como:

a) “Cross-site scripting” que consiste en la inclusión de código script malicioso en el cliente que consulta el servidor web.

b) “SQL injection” que consiste en introducir un código SQL que vulnere la Base de Datos de nuestro servidor.

c) “Denial-of-service” que consiste en que el servidor de aplicación sea incapaz de servir peticiones correctas de usuarios.

Algunos sistemas WAF existentes en el mercado también monitorizan las respuestas del servidor, por ejemplo, si en una respuesta, que el servidor web envía al usuario se detectan cadenas que pueden ser identificadas como cuentas bancarias, el WAF lo puede detectar como un posible ataque y denegar la respuesta.

ANEXO A.2.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA BÁSICA DEL ENS PARA SERVIDORES IIS 10 SOBRE MICROSOFT WINDOWS SERVER 2016 EN ENTORNO DE DOMINIO

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores IIS 10 sobre Microsoft Windows Server 2016 con implementación de seguridad de categoría básica del ENS.

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

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar la sección de la guía "ANEXO A.2.1 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 MIEMBROS DEL DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS"

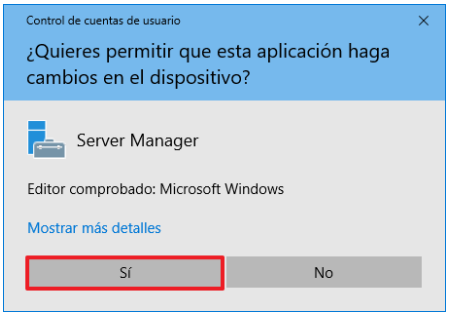
1. COMPROBACIONES EN CONTROLADOR DE DOMINIO

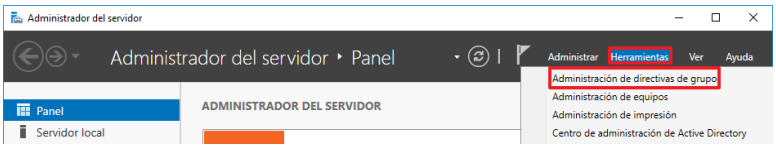
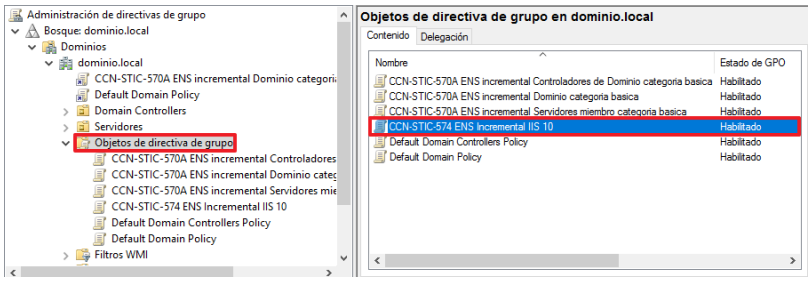
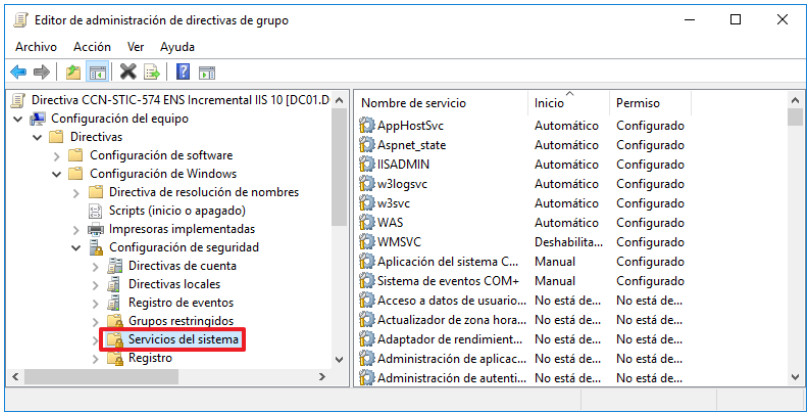
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador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

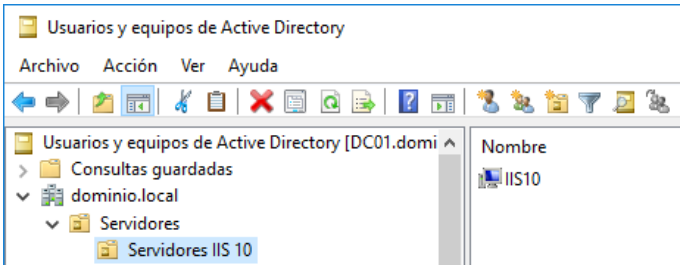
a) Usuarios y equipos de Active Directory (dsa.msc).

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

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

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio.		Inicie sesión con una cuenta que tenga privilegios de administración del dominio. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Pulse "Sí" en la ventana de "Control de cuentas de usuario". 

Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que los objetos de directivas de grupo han sido creados y están habilitados.		Ejecute la herramienta "Administrador de directivas de grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"**  Dentro de la consola diríjase a los "Objetos de directiva de grupo": "**Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo**" Verifique que está creado el objeto de directiva de grupo "CCN-STIC-574 ENS Incremental IIS 10", y que en la columna "Estado de GPO" figura como habilitada. 
3. Verifique los valores de los servicios del sistema de la directiva CCN-STIC-574 ENS Incremental IIS 10		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-574 ENS Incremental IIS 10" tiene los siguientes valores de servicios de sistema dentro de: **"Directiva CCN-STIC-574 ENS Incremental IIS 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"**. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="4">Cómo hacerlo</th></tr>
<tr><th colspan="2">Servicio (nombre largo)</th><th>Servicio (nombre corto)</th><th>Inicio</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td colspan="2">Servicio auxiliar de host para aplicaciones</td><td>AppHostSvc</td><td>Automático</td><td></td><td></td></tr>
<tr><td colspan="2">ASP.NET State Service</td><td>Aspnet_state</td><td>Automático</td><td></td><td></td></tr>
<tr><td colspan="2">Aplicación del sistema COM+</td><td>COMSysApp</td><td>Manual</td><td></td><td></td></tr>
<tr><td colspan="2">Servicio de administración IIS</td><td>IISADMIN</td><td>Automático</td><td></td><td></td></tr>
<tr><td colspan="2">Servicio de registro de W3C</td><td>w3logsvc</td><td>Automático</td><td></td><td></td></tr>
<tr><td colspan="2">Servicio de publicación World Wide Web</td><td>w3svc</td><td>Automático</td><td></td><td></td></tr>
<tr><td colspan="2">Servicio WAS</td><td>WAS</td><td>Automático</td><td></td><td></td></tr>
<tr><td colspan="2">Servicio de Administración Web</td><td>WMSVC</td><td>Manual</td><td></td><td></td></tr>
<tr><td>4. Verifique que los servidores de IIS 10 están dentro de las Unidades Organizativas correspondientes</td><td></td><td colspan="4">Utilice la herramienta Usuarios y equipos de Active Directory (“Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory”) y seleccione las unidades organizativas que contienen los Servidores IIS 10.
Nota: Para el desarrollo de esta guía se utiliza la Unidad Organizativa “Servidores IIS 10”.
 
</td></tr>
</table>

2. COMPROBACIONES EN SERVIDOR MIEMBRO

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

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

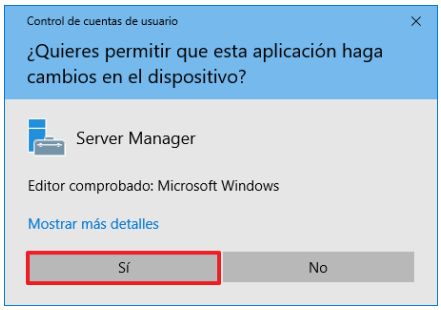
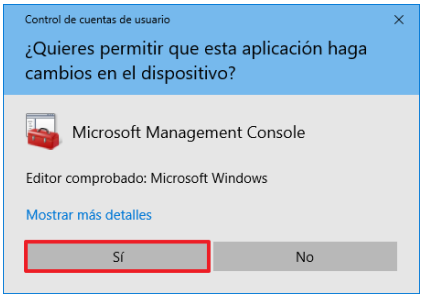
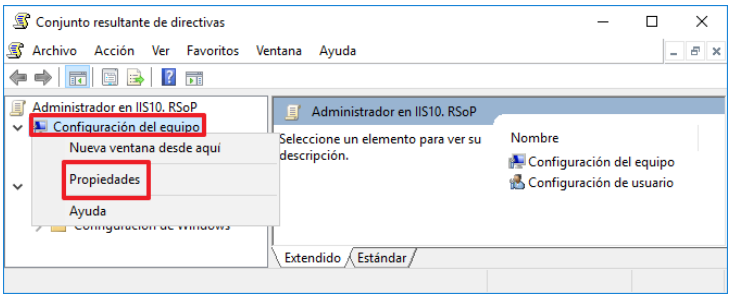
a) Administrador del Servidor

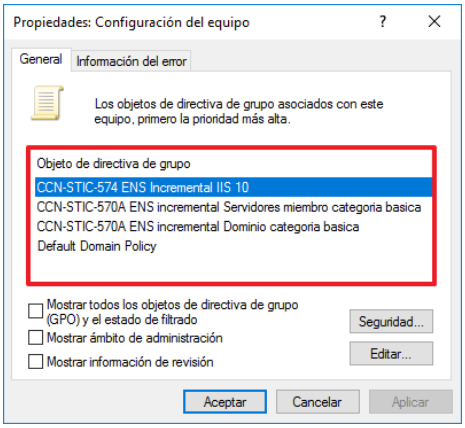
b) Conjunto resultante de directivas (rsop.msc)

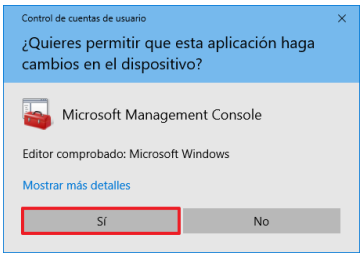
c) Consola de servicios (services.msc)

d) Editor de registro (regedit.exe)

e) Explorador de Archivos (explorer.exe)

Comprobación	OK/NOK	Cómo hacerlo
5. Inicie sesión en el servidor a comprobar.		En uno de los servidores miembro del dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Pulse "Sí" en la ventana de "Control de cuentas de usuario". 
6. Verifique que el equipo ha recibido la directiva de grupo CCN-STIC-574 ENS incremental IIS 10		Ejecute la consola de administración "Conjunto resultante de directivas", para ello, pulse **"Tecla Windows+R → rsop.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" en la ventana que se muestra a continuación.  Seleccione en ella la rama "Configuración del equipo", márquela con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la figura. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", resaltada en la siguiente figura.
 

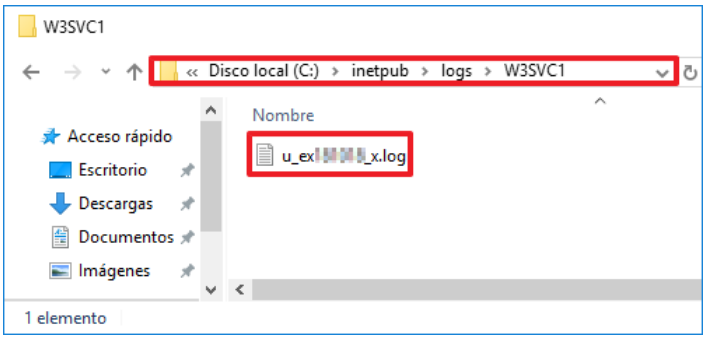
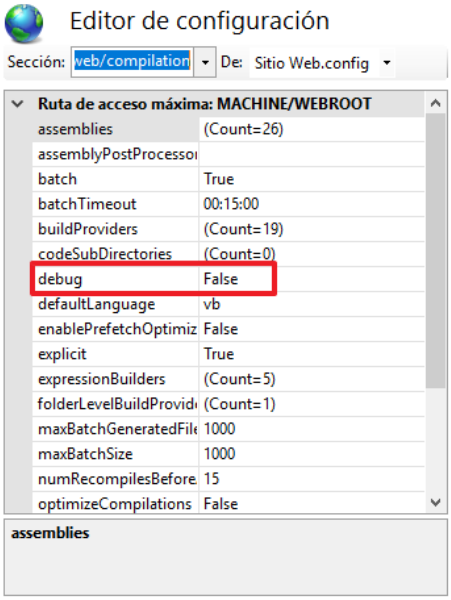
Verifique que en dicha sección aparecen listados, y por ese orden, los objetos de directiva de grupo que se indican en la siguiente tabla:</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Regla de entrada</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-574 ENS incremental IIS 10.0</td><td></td></tr>
<tr><td>CCN-STIC-570 ENS incremental Servidores miembro categoria basica</td><td></td></tr>
<tr><td>CCN-STIC-570 ENS incremental Dominio categoria basica</td><td></td></tr>
<tr><td>Default Domain Policy</td><td></td></tr>
</table></td></tr>
<tr><td>7. Verifique que los servicios del sistema están correctamente configurados</td><td></td><td>Usando la consola de servicios (el sistema solicitará elevación de privilegios):
“Tecla Windows+R → services.msc”
El Control de cuentas de usuario solicitará elevación de privilegios. Pulse “Sí” para continuar.
 

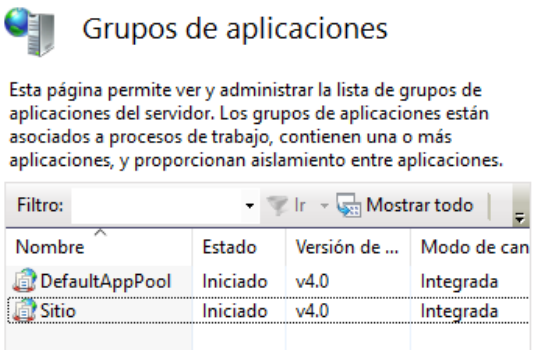
Verifique que el tipo de inicio de los servicios que aparecen en el sistema y en la siguiente tabla coinciden:
Nota: Dependiendo de las características de IIS 10 instaladas en el equipo es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales.</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio auxiliar de host para aplicaciones		AppHostSvc	Automático		
ASP.NET State Service		Aspnet_state	Automático		
Aplicación del sistema COM+		COMSysApp	Manual		
Servicio de administración IIS		IISADMIN	Automático		
Servicio de registro de W3C		w3logsvc	Automático		
Servicio de publicación World Wide Web		w3svc	Automático		
Servicio WAS		WAS	Automático		
Servicio de Administración Web		WMSVC	Manual		

8. Verifique que se han asignado los permisos correctos en el sistema de archivos		Utilizando el Explorador de Windows: **"Windows+R → Explorer"** En caso de no saber dónde apunta cada una de las rutas abreviadas que se especifica, ejecute Explorer <<ruta>> donde <<ruta>> se sustituirá por la ruta abreviada. **Nota:** Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, marcándolo con el botón derecho y eligiendo la opción "Propiedades" del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá situarse en la pestaña "Seguridad". En la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios. Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados.

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\System32\inetsrv\MetaBack	Administrador	Control total	
	System	Control total	
%SystemRoot%\System32\LogFiles	Administradores	Control Total	
	SYSTEM	Control Total	
	Creator Owner	Control Total	

Comprobación	OK/NOK	Cómo hacerlo
9. Compruebe que el registro de acceso de IIS está operativo.		En la configuración que ha realizado ha habilitado el registro de acceso al servidor, por lo que debe asegurarse que está registrando la actividad. Para ello verifique que el directorio **C:\inetpub\logs\W3SVC1** contiene ficheros con el formato **u_ex*fecha*.log**. Abriendo el último deberá ver que registra los accesos correctamente.  **Nota:** Tenga en cuenta que no se crea ningún registro hasta que no se realiza alguna actividad.
10. Comprobación de la depuración de sistemas en producción.		Compruebe que la depuración en sistemas de producción esta deshabilitada. Para ello chequee: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS) → [nombre_del_servidor]→ Sitios → Editor de configuración> Sección: System.web>Compilation → Debug.→ False"**. 

Comprobación	OK/NOK	Cómo hacerlo
11. Comprobación de las identidades del grupo de aplicaciones.		Compruebe que en las identidades del grupo de aplicaciones no hay identidades de servicio integradas. Para ello chequee: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS)→ [nombre_del_servidor] → Grupo de aplicaciones"**. 

ANEXO A.2.3. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 INDEPENDIENTES SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

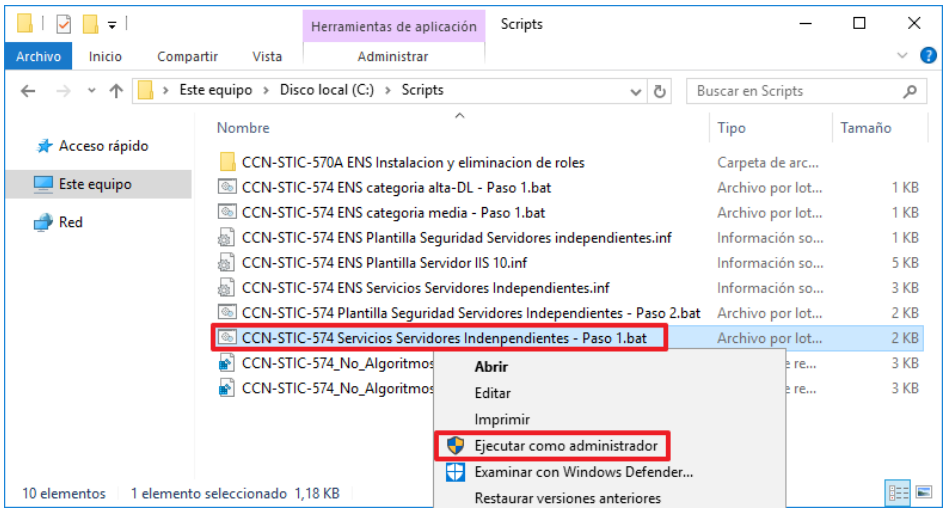
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tenga que securizar IIS 10 sobre Windows Server 2016 independientes con una categorización de seguridad básica según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría básica, deberá realizar las implementaciones según se referencian en el presente anexo.

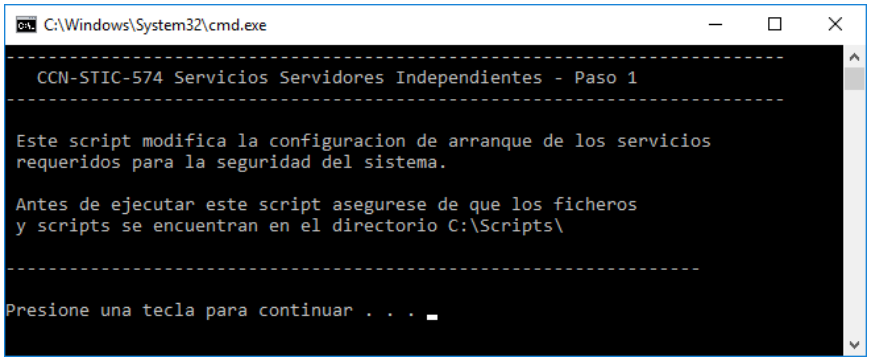
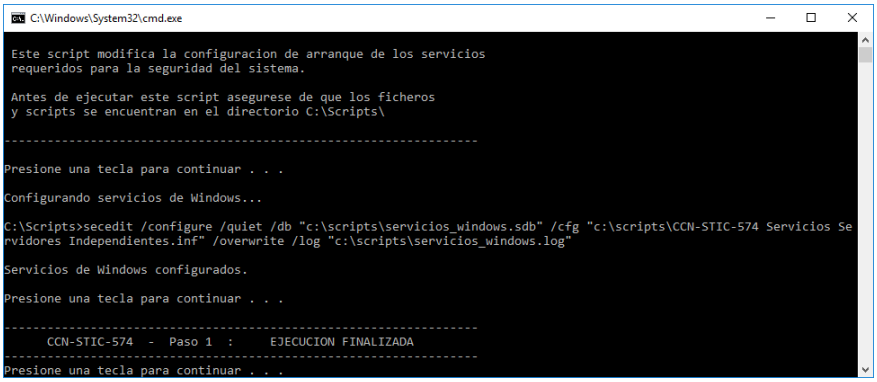
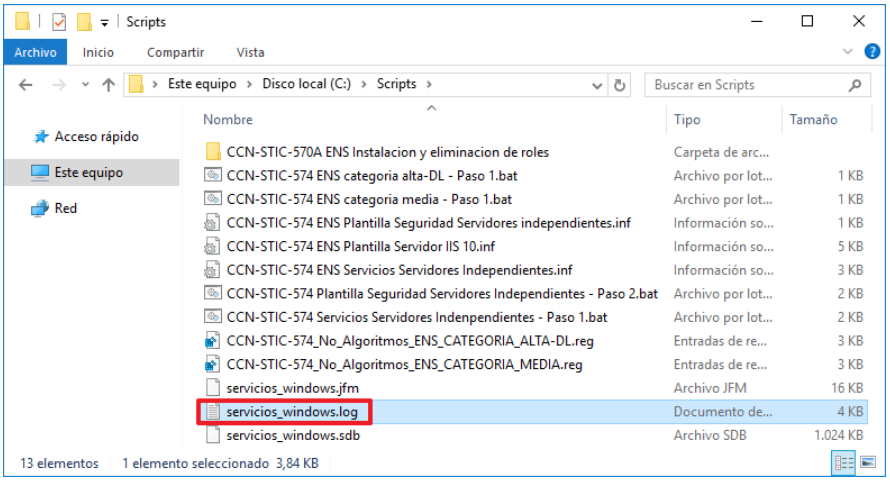
Debe tener en consideración que, antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

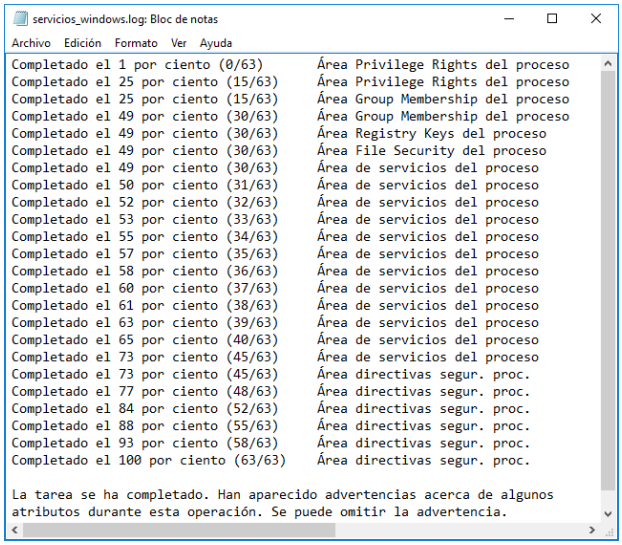
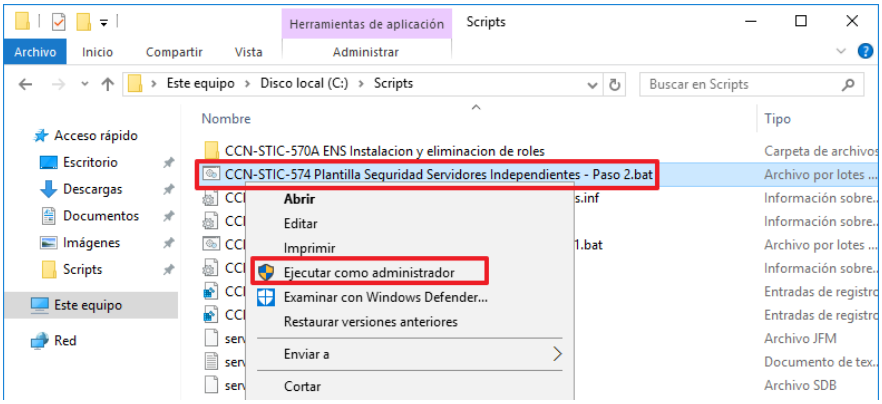
Nota: Si instala Internet Information Services por primera vez con la guía 570A o 570B aplicada debe habilitar la instalación remota de roles, características y servicios de rol a través de Shell la cual se encuentra deshabilitada por LGPO.
Si ha instalado el rol de IIS después de haber aplicado el procedimiento descrito en las guías mencionadas anteriormente, deberá volver a aplicar dicho paso a paso antes de continuar con la presente guía. Esto es debido a que durante la instalación del rol se modifican los permisos de usuario del sistema y altera el nivel mínimo de seguridad establecido por el ENS.

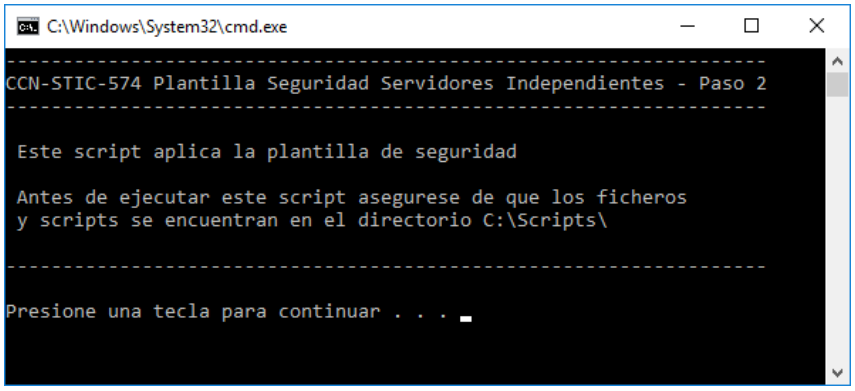
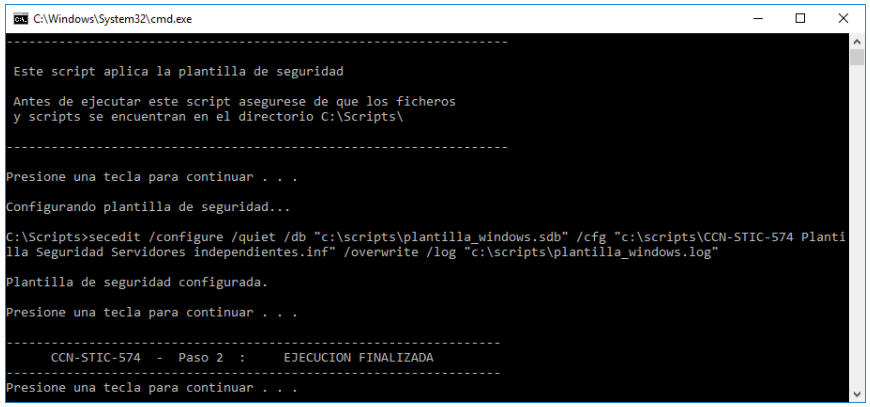
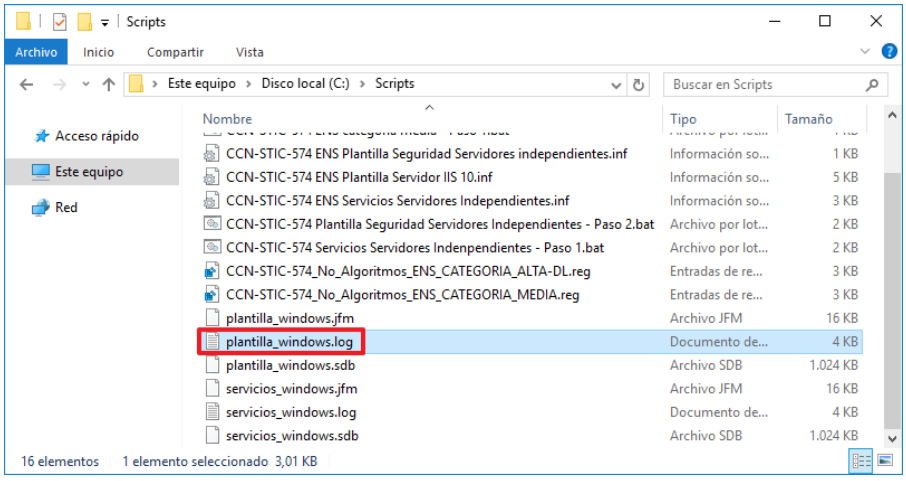
1. CONFIGURACIÓN DE LA SEGURIDAD LOCAL

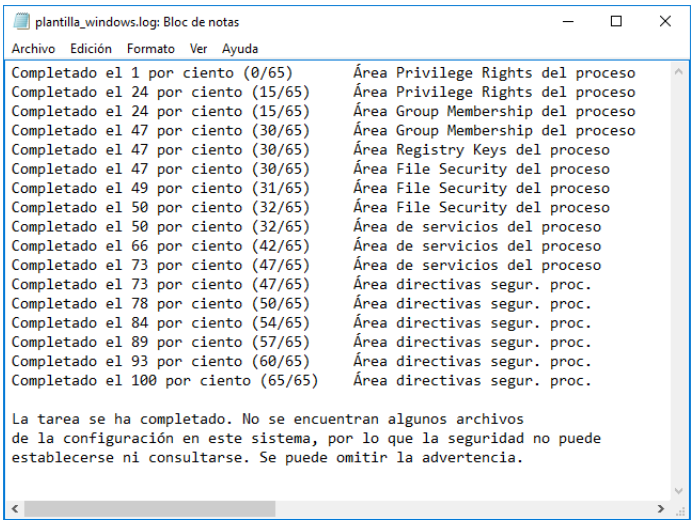
Los pasos que se describen a continuación se realizarán en todos aquellos servidores IIS 10 sobre Microsoft Windows Server 2016, independientes, que implementen servicios o información de categoría básica y que se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

Paso	Descripción
1.	Inicie sesión en el servidor independiente donde se va aplicar seguridad según criterios de ENS. 
2.	Debe iniciar sesión con una cuenta que sea Administrador del servidor.
3.	Cree el directorio “Scripts” en la unidad “C:\”.
4.	Copie los scripts asociados a esta guía en el directorio “C:\Scripts”.
5.	Abra la carpeta “C:\Scripts” y pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-574 Servicios Servidores Independientes – Paso 1.bat” y seleccione la opción “Ejecutar como administrador”.  **Nota:** En función del usuario con el que se haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que se le solicite la elevación de privilegios. Para ello introduzca las credenciales de un usuario con permisos de administrador o bien eleve automáticamente los privilegios sin necesidad de introducir usuario y contraseña.

Paso	Descripción
6.	Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la categoría básica del ENS. 
7.	Una vez completado el proceso, deberá pulsar una tecla para continuar. 
8.	Pulse de nuevo otra tecla, para finalizar la ejecución del script. La ejecución del script genera un registro en la carpeta “C:\Scripts” con el nombre de “servicios_windows.log”. 

Paso	Descripción
9.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación. 
10.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-574 Plantilla Seguridad Servidores Independientes - Paso 2.bat” y seleccione la opción “Ejecutar como administrador”.  **Nota:** En función del usuario con el que se haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que se le solicite la elevación de privilegios. Para ello introduzca las credenciales de un usuario con permisos de administrador o bien eleve automáticamente los privilegios sin necesidad de introducir usuario y contraseña.

Paso	Descripción
11.	Pulse una tecla para iniciar la ejecución del script que configurará la plantilla de seguridad con la seguridad requerida para la categoría básica del ENS. 
12.	Una vez completado el proceso, deberá pulsar una tecla para continuar. 
13.	Pulse de nuevo otra tecla, para finalizar la ejecución del script. La ejecución del script genera un registro en la carpeta “C:\Scripts” con el nombre de “plantilla_windows.log”. 

Paso	Descripción
14.	Abra este registro para comprobar si la configuración de la plantilla ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación. 

2. CONFIGURACIONES ESPECIFICAS DE LA ORGANIZACIÓN

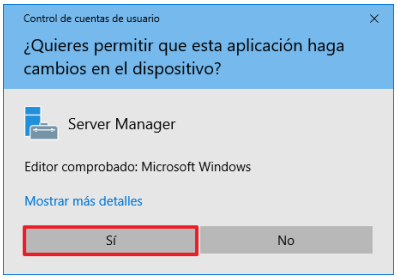
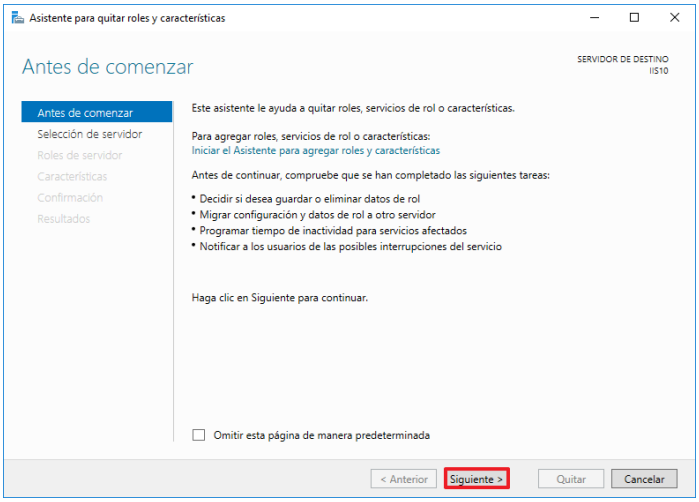
El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto,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

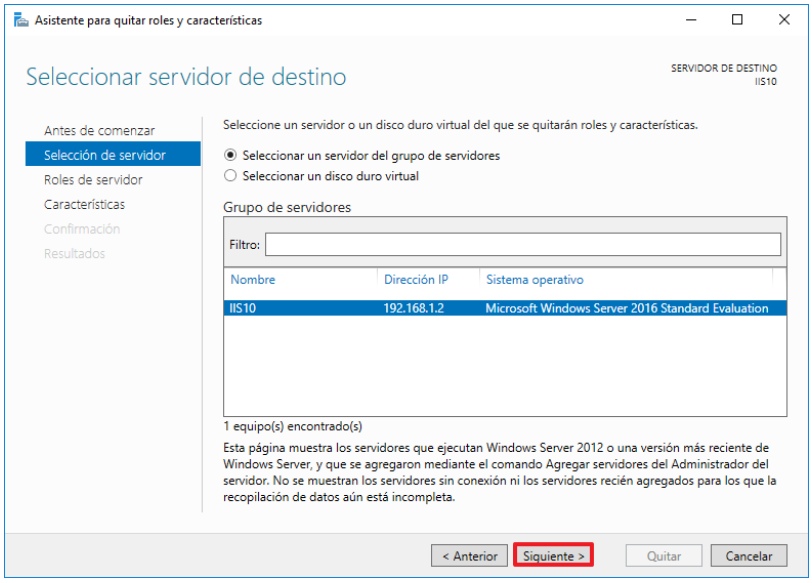
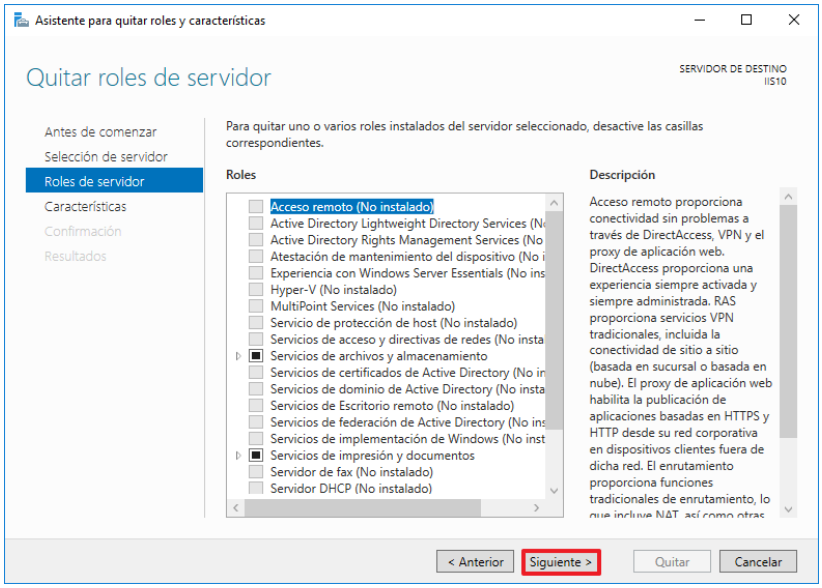
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

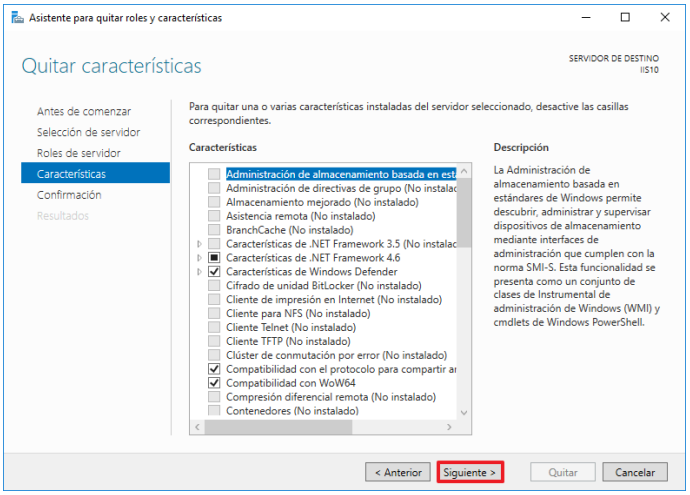
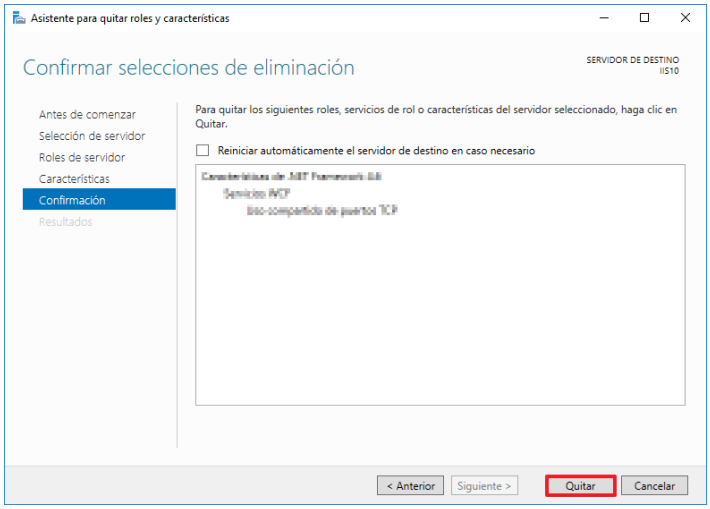
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

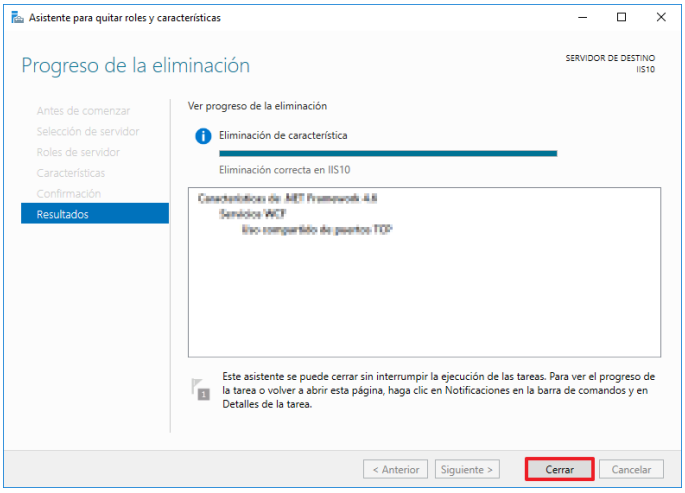
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

Es recomendable que el sitio web este alojado en otra ubicación de disco diferente a la del sistema operativo y que esta solo se utilice para el alojamiento de sitios web, evitando con ello exponer más información de la estrictamente necesaria.

Paso	Descripción
15.	A continuación, deberá iniciar sesión en el servidor independiente donde está instalado el rol de IIS 10.
16.	Pulse sobre el administrador del servidor. 
17.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 
18.	A continuación, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione **“Administrar→ Quitar roles y funciones”**. 
19.	Comenzará el asistente para quitar roles y características, pulse sobre el botón “Siguiente >”. 

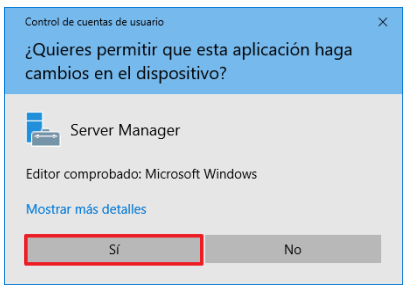
Paso	Descripción
20.	Seleccione el servidor donde desea quitar las características del IIS 10 y pulse siguiente. 
21.	En la siguiente ventana podrá quitar roles del servidor, en este caso pulse siguiente para acceder a las características de los roles instalados. 

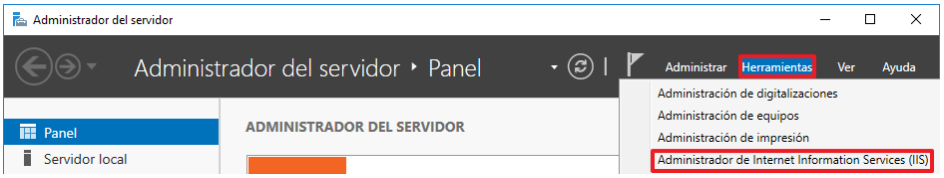
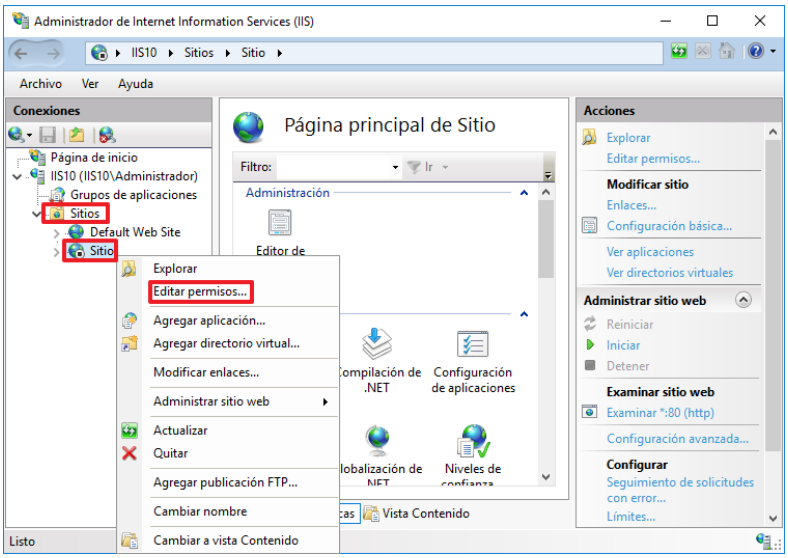
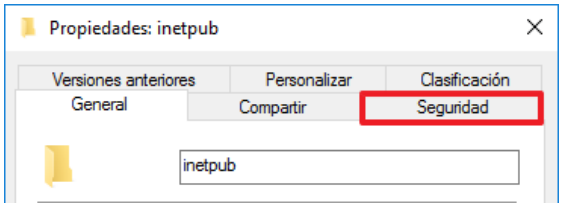
Paso	Descripción
22.	A continuación, seleccione las características que desea quitar. 
23.	La siguiente pantalla mostrara las características a modos resumen que desea quitar, confirme que las características seleccionadas son las correctas y pulse “Quitar”. 

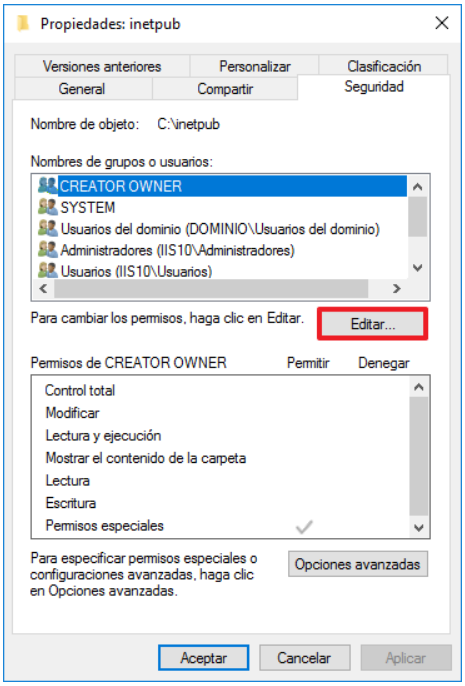
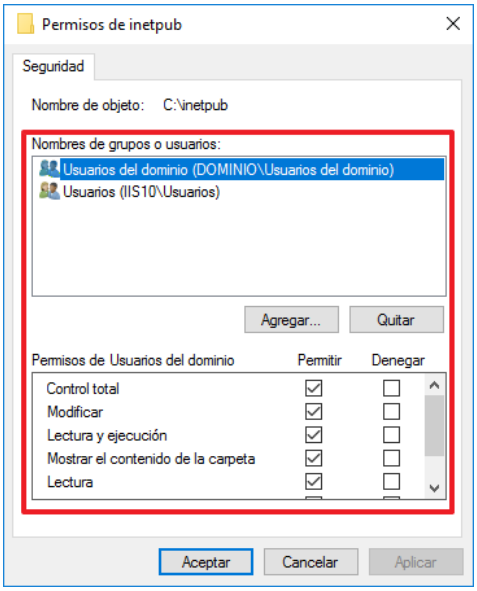
Paso	Descripción
24.	Una vez finalizada la desinstalación pulse “Cerrar”.  **Nota:** Debe tener en cuenta que la desinstalación de determinadas características puede requerir el reinicio del equipo.

2.2. GESTION DE PERMISOS RECURSOS WEB

En este apartado se tendrá en consideración la gestión y administración del acceso a los recursos web según el marco operacional de categoría básica establecido por el ENS, para con ello limitar y controlar el acceso a directorios con información sensible de ser sustraída.

Paso	Descripción
25.	Inicie sesión en el servidor independiente donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
26.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 

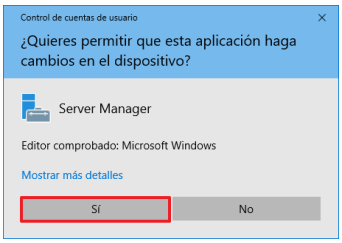
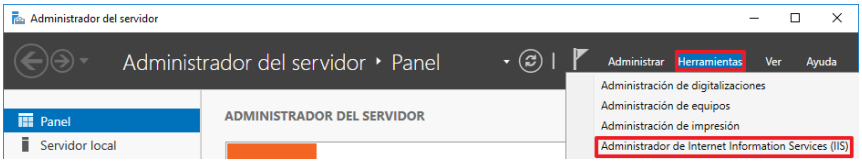
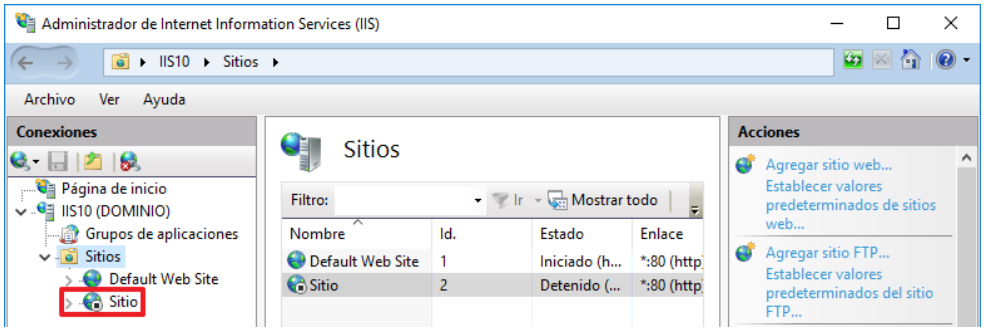
Paso	Descripción
27.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”** 
28.	Pulse botón derecho sobre el sitio al cual quiere asignar o quitar permisos. 
29.	Diríjase hasta la pestaña seguridad. 

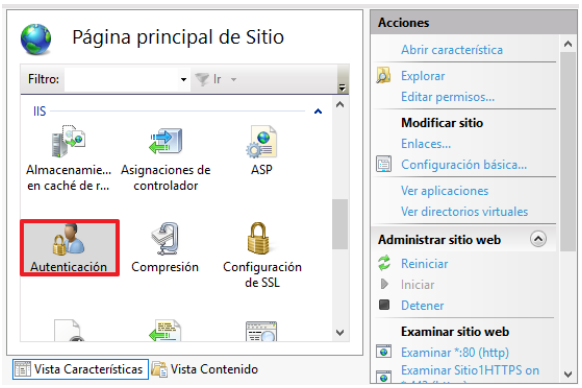
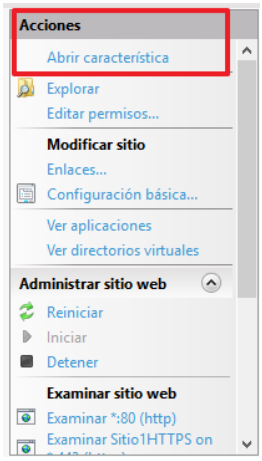
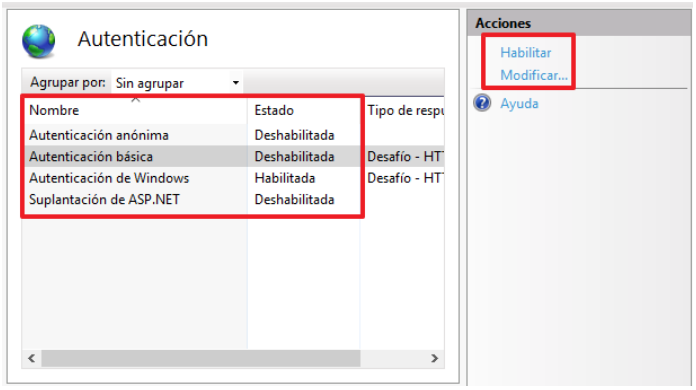
Paso	Descripción
30.	A continuación, pulse el botón “Editar”. 
31.	A continuación, seleccione los permisos del que desea establecer para ese sitio web.  **Nota:** Es recomendable dar permiso solo a los usuarios o grupos que deban tener acceso al sitio web evitando que el usuario administrador tenga permiso para prevenir posibles vulnerabilidades.

2.3. AUTENTICACIÓN SITIO WEB

Los métodos de autenticación permitirán limitar el acceso al sitio web a una lista determinada de usuarios (el método habilitado por defecto de los servicios web de IIS es la autenticación anónima), en la categoría básica y media de seguridad se debe limitar el acceso al contenido web a usuarios anónimos para prevenir posibles ataques.

Los siguientes pasos indican cómo deshabilitar la autenticación anónima a nivel de sitio Web.

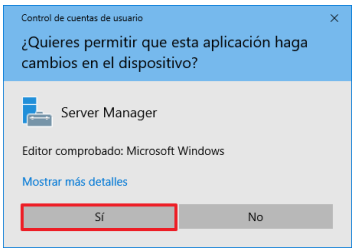
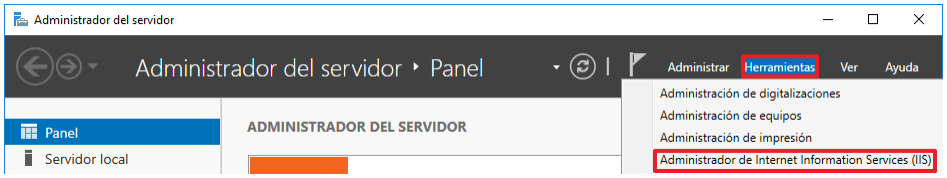
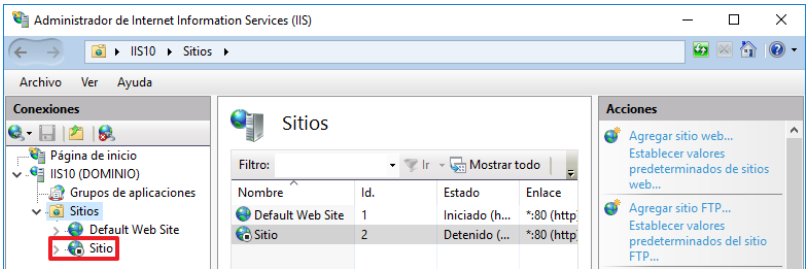
Paso	Descripción
32.	Inicie sesión en el servidor independiente donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
33.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar. 
34.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”** 
35.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo “Conexiones” y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.

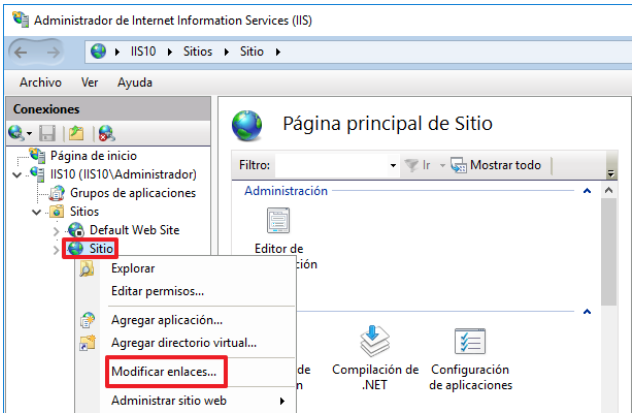
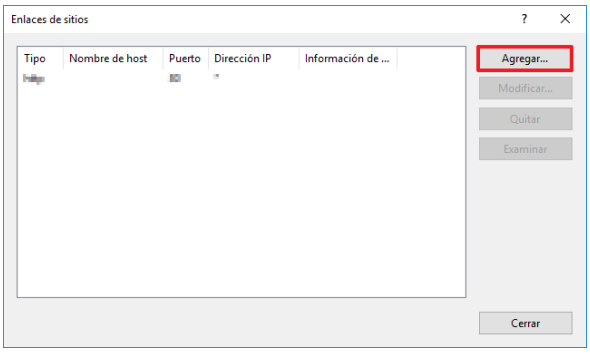
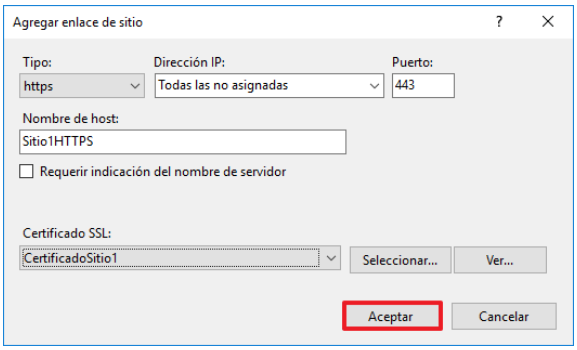
Paso	Descripción
36.	Seleccione en la página principal del sitio web el icono de “Autenticación”. 
37.	Pulse sobre “Abrir característica” situado en el panel derecho en el menú “Acciones”. 
38.	A continuación, establezca según las características de su organización los métodos de autenticación disponibles. Para ello pulse sobre el método de autenticación que quiere configurar y en el panel derecho seleccione la acción que desea realizar.  **Nota:** Únicamente se usará la autenticación anónima para páginas webs generales en la que solo se muestre contenido y no sea necesaria la autenticación del usuario.

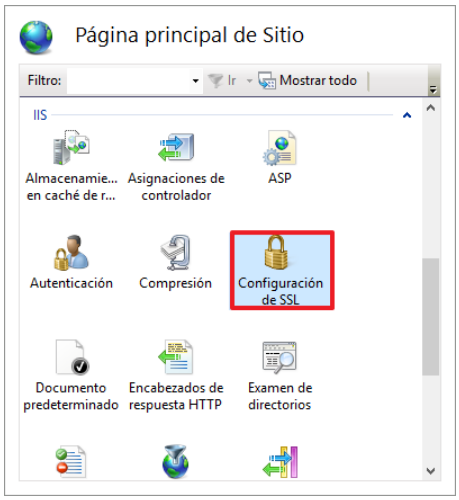
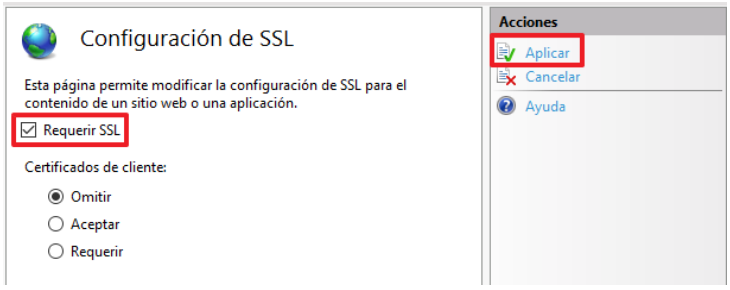
2.4. CERTIFICADOS

IIS 10 faculta el empleo de protocolos seguros para las comunicaciones y los procesos de autenticación usando HTTPS que utiliza un cifrado basado en SSL/TLS para crear un canal cifrado para el tráfico de información sensible,

Para sitios públicos es recomendable el uso de certificados emitidos por CA de terceros reconocidas, en el caso de sitios web internos es recomendable el uso de una entidad certificadora interna, desaconsejando el uso de certificados autofirmados.

Paso	Descripción
39.	Inicie sesión en el servidor independiente donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
40.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar. 
41.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”** 
42.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo de “Conexiones” y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.

Paso	Descripción
43.	Pulse con el botón derecho sobre el sitio web que quiere modificar y seleccione la opción “Modificar enlaces…”. 
44.	Pulse sobre el botón “Agregar…”. 
45.	Seleccione Tipo: “Https”, selecciones Certificado SSL: “CertificadoSitio1” y pulse “Aceptar”.  **Nota:** “CertificadoSitio1” es un certificado creado para este ejemplo, debe usar el correspondiente para su organización.

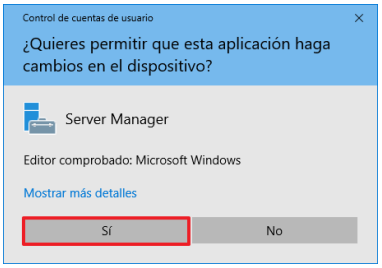
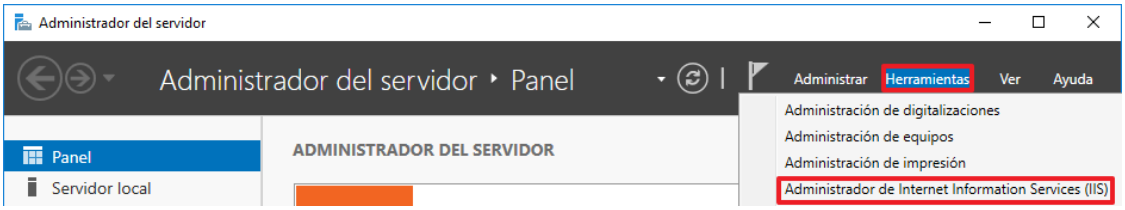
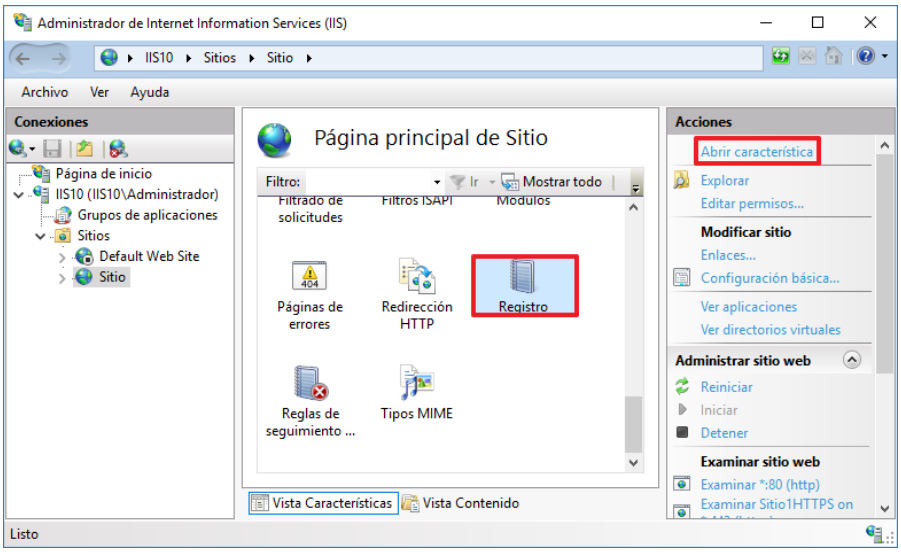
Paso	Descripción
46.	A continuación, deberá configurar el sitio web para que los usuarios requieran un certificado propio, para ello pulse sobre en el sitio web que desea configurar, y seleccione “Configuración de SSL”: 
47.	Seleccione la opción de “Requerir SSL” y pulse sobre “Aplicar” para que el sistema guarde los cambios realizados. 

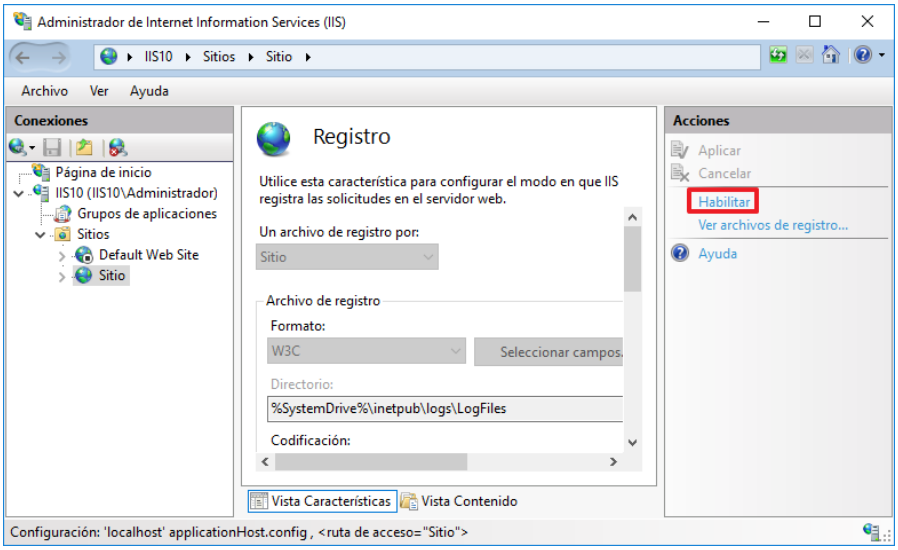
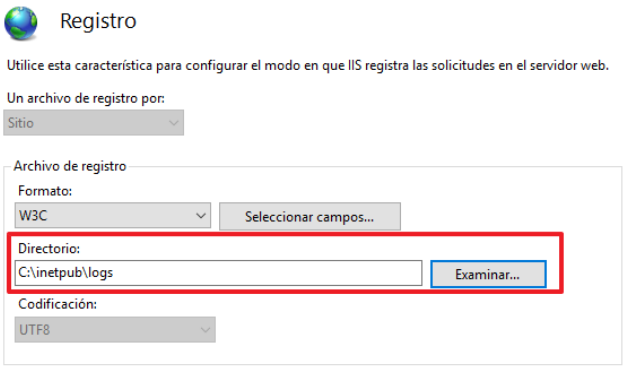
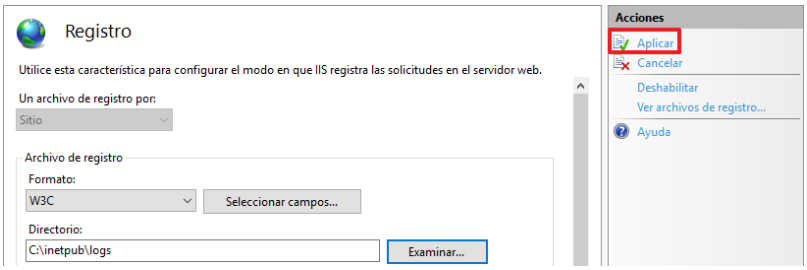
2.5. AUDITORÍA

Con la aplicación del ENS para la categoría básica sobre IIS 10 quedará registrado el uso del sistema para poder detectar y reaccionar a cualquier fallo accidental o deliberado, quedando registrado en el sistema quien realiza la actividad, cuando y sobre qué información con el fin de detectar anomalías o intentos frustrados de acceso a información no autorizada.

La ubicación de los registros debe ser diferente a la del sistema además de tener limitado el acceso únicamente a los usuarios autorizados.

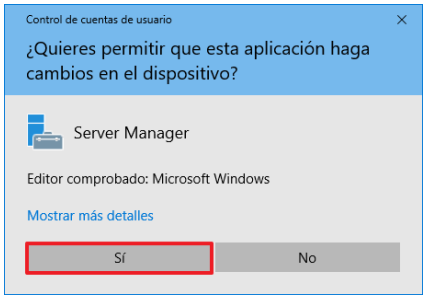
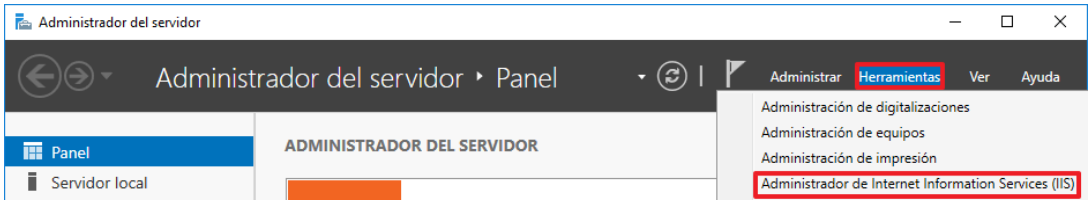
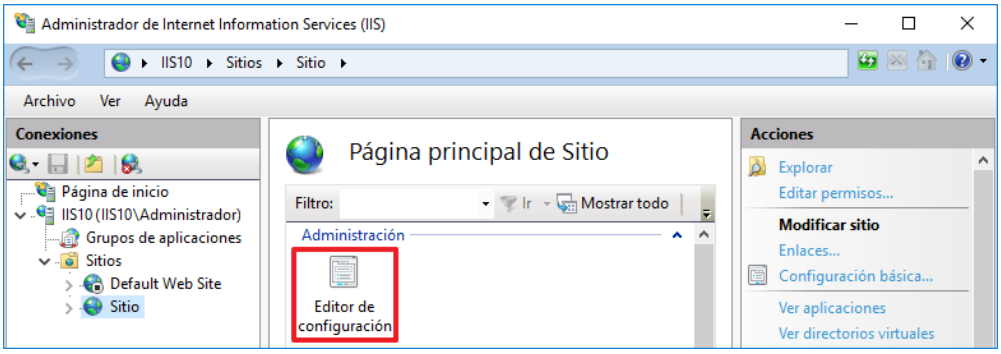
Paso	Descripción
48.	Inicie sesión en el servidor independiente donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 

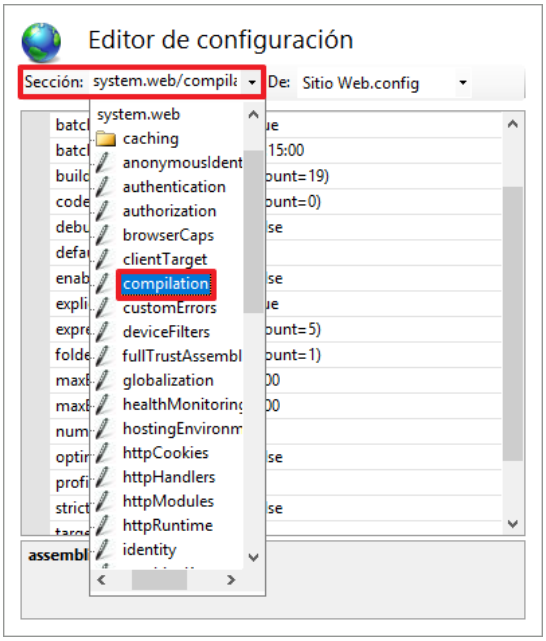
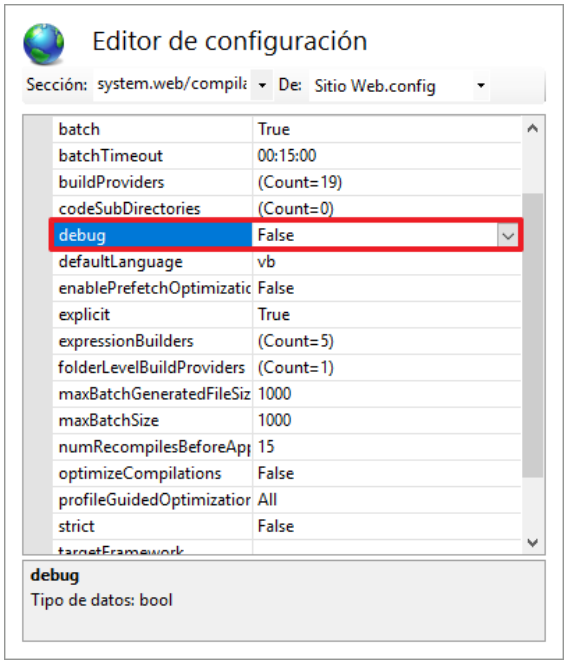
Paso	Descripción
49.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 
50.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”** 
51.	Diríjase al sitio web que desea administrar, a continuación, localice el icono “Registro”, y pulse la acción “Abrir característica” situado en la parte superior derecha de la pantalla para acceder a la configuración del registro. 

Paso	Descripción
52.	Debe habilitar el registro de las solicitudes del servidor IIS 10 para ello, diríjase al menú “Acciones” situado en la parte superior derecha de la pantalla y pulse sobre “Habilitar”. 
53.	A continuación, seleccione el directorio donde se van a guardar los registros, por seguridad es recomendable realizarlo en una unidad diferente a la de la instalación del sistema operativo. 
54.	Una vez realizados los cambios deberá guardarlos, para ello pulse “Aplicar” situado en el menú “Acciones” en la parte superior izquierda de la pantalla. 

2.6. DESHABILITAR MODOS DE DEPURACIÓN

El siguiente paso define el procedimiento para la modificación del fichero web.config para inhabilitar el modo de depuración de una aplicación en entornos de producción, evitando con ello posibles fisuras de seguridad.

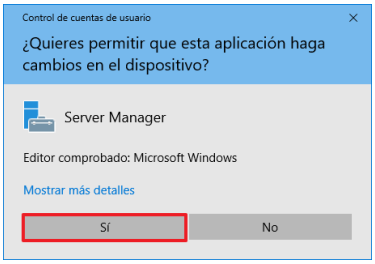
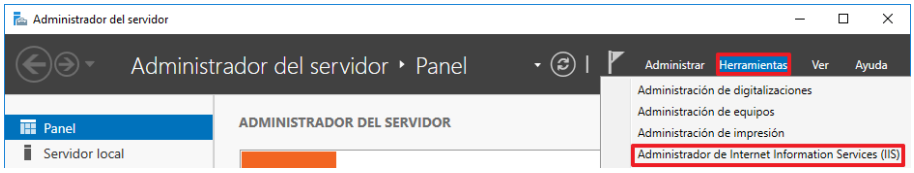
Paso	Descripción
55.	Inicie sesión en el servidor independiente donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
56.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar. 
57.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”** 
58.	Localice el sitio web que desea configurar y seleccione “Editor de configuración”, a continuación, pulse en el menú “Acciones” la opción “Abrir característica” situado en la parte superior derecha de la pantalla para abrir el editor de configuración. 

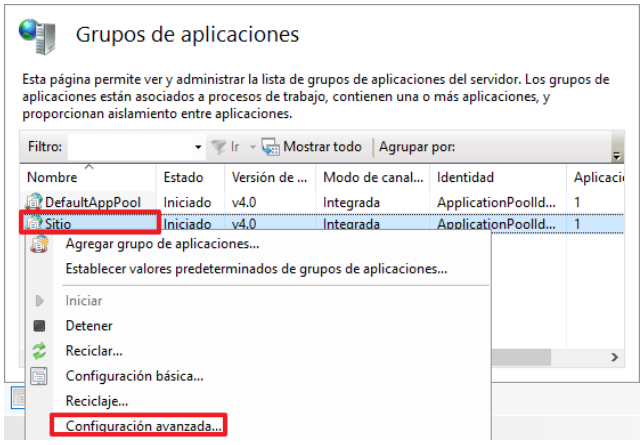
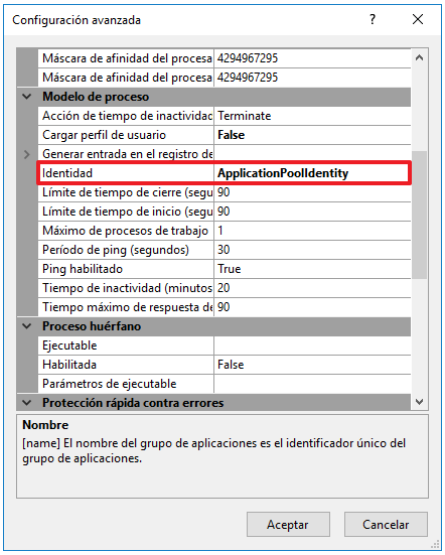
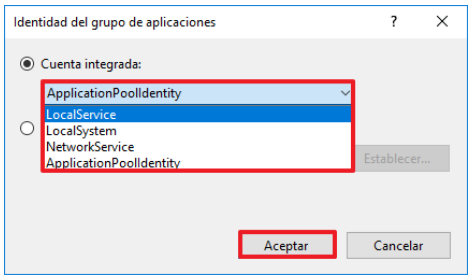
Paso	Descripción
59.	Navegue en “Sección” hasta “system.web/compilation”. 
60.	Localice la opción “Debug”, abra el desplegable y seleccione “False”. 

2.7. IDENTIDADES DEL GRUPO DE APLICACIONES

El siguiente paso define el procedimiento para la modificación de las identidades de una aplicación las cuales deben modificarse con la aplicación del ENS para la categoría básica sobre IIS 10 y evitando el uso de identidades de servicio integradas tales como servicio local o sistema local.

Para una mayor seguridad los grupos de aplicaciones deben ejecutarse bajo la identidad del grupo cuando se crea el grupo de aplicaciones, el valor predeterminado y más seguro es "ApplicationPoolIdentity". El uso de una cuenta personalizada es aceptable, pero debe asegurarse de usar una cuenta diferente para cada grupo de aplicaciones.

Paso	Descripción
61.	Inicie sesión en el servidor independiente donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
62.	El sistema solicitará elevación de privilegios. Pulse sobre el botón "Sí" para confirmar. 
63.	Inicie la herramienta "Administrador de Internet Information Services (IIS)". Para ello, pulse sobre el menú superior de la derecha de la herramienta "Administrador del servidor" y seleccione **"Herramientas → Administrador de Internet Information Services (IIS)"** 
64.	Despliegue el servidor y seleccione la opción "Grupos de aplicaciones". 

Paso	Descripción
65.	A continuación, seleccione la aplicación que desea configurar y haga clic botón derecho sobre ella y pulse “Configuración avanzada…”. 
66.	Localice la opción “Identidad” dentro de “Modelo de proceso”. 
67.	A continuación, seleccione la opción que más se adecue a sus necesidades y pulse aceptar. 

2.8. LIMPIEZA DE METADATOS

Se ha de tener en consideración que en un servidor web se pueden alojar documentos que pueden contener información oculta en los metadatos los cuales contienen información que permite catalogar, ordenar y clasificar nuestros archivos, por lo que pueden ser un riesgo de seguridad para nuestra organización, por lo que hay que tener especial atención en la limpieza de los metadatos de los documentos que se alojan en el servidor web por ello antes de alojar un fichero en el servidor web se ha debido de realizar el procedimiento indicado en MP. INFO. 6. LIMPIEZA DE DOCUMENTOS.

En el proceso de limpieza se ha de tener en consideración que se retiraran todos los datos de los documentos además de la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, con la excepción de la información pertinente para el receptor del documento.

2.9. SOLUCIONES WAF (WEB APLICATION FIREWALL)

Un servidor web puede alojar aplicaciones por lo que es importante un control exhaustivo de estas por ello se han de emplear uno de los elementos principales en la protección de entornos de aplicaciones Web que son los cortafuegos (firewalls) de aplicaciones Web, también conocidos como WAF, Web Application Firewall.

El WAF se encargará de proteger los servidores de aplicaciones web de determinados ataques específicos en Internet además de controlar las transacciones al servidor web de nuestra organización.

Este sistema nos permite evitar probables ataques como:

a) “Cross-site scripting” que consiste en la inclusión de código script malicioso en el cliente que consulta el servidor web.

b) “SQL injection” que consiste en introducir un código SQL que vulnere la Base de Datos de nuestro servidor.

c) “Denial-of-service” que consiste en que el servidor de aplicación sea incapaz de servir peticiones correctas de usuarios.

Algunos sistemas WAF existentes en el mercado también monitorizan las respuestas del servidor, por ejemplo, si en una respuesta, que el servidor web envía al usuario se detectan cadenas que pueden ser identificadas como cuentas bancarias, el WAF lo puede detectar como un posible ataque y denegar la respuesta.

ANEXO A.2.4. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA BÁSICA DEL ENS PARA SERVIDORES IIS 10 SOBRE MICROSOFT WINDOWS SERVER 2016

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar la sección de la guía "ANEXO A.2.3 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 INDEPENDIENTES SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS".

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores IIS 10 sobre Microsoft Windows Server 2016 independiente con implementación de seguridad de categoría básica del ENS.

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

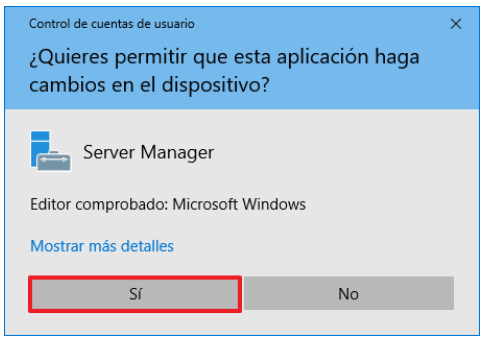
Para realizar las comprobaciones pertinentes en los servidores independientes se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor. Las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

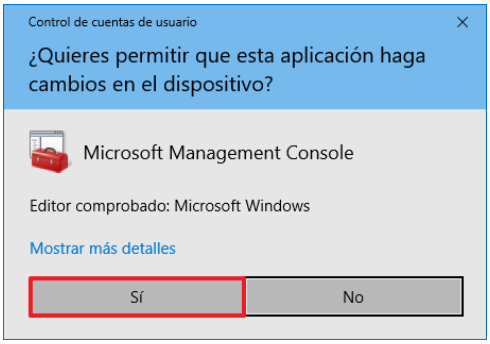
a) Administrador del Servidor

b) Consola de servicios (services.msc)

c) Editor de registro (regedit.exe)

d) Explorador de Archivos (explorer.exe)

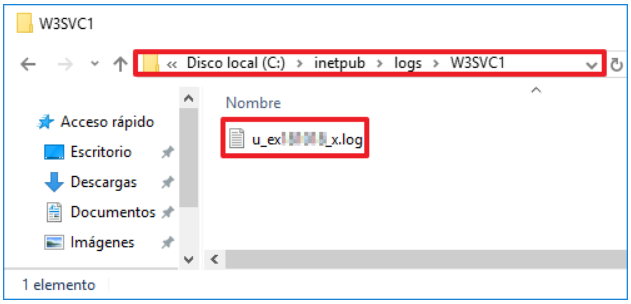
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un servidor independiente		En uno de los servidores independientes, inicie sesión con una cuenta que tenga privilegios de administración. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Pulse "Sí" en la ventana de "Control de cuentas de usuario". 

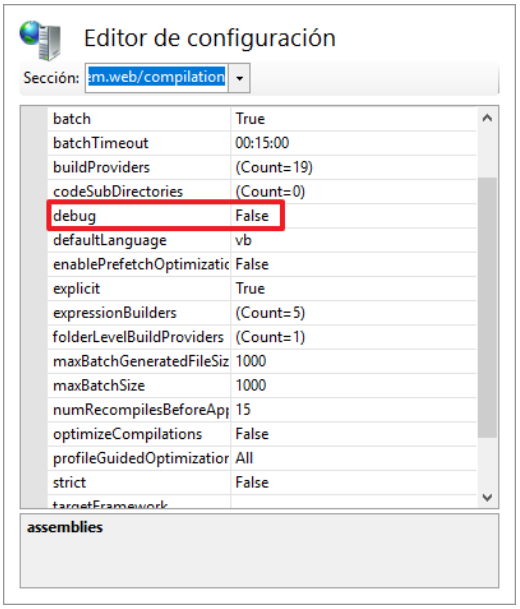
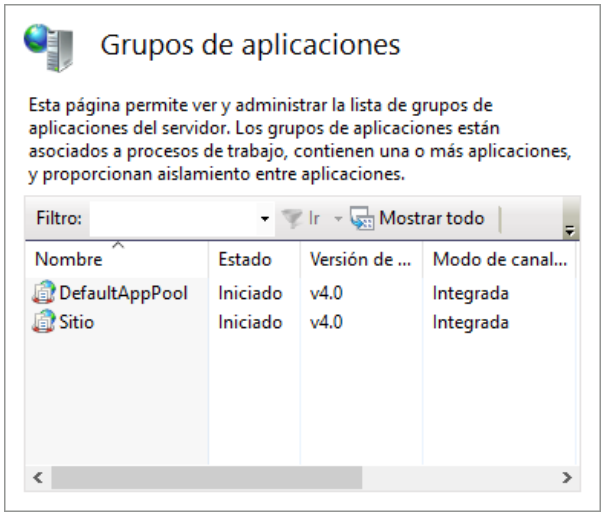
Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que los servicios del sistema están correctamente configurados		Usando la consola de servicios (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → services.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" para continuar.  Verifique que el tipo de inicio de los servicios que aparecen en el sistema y en la siguiente tabla coinciden: **Nota:** Dependiendo de las características de IIS 10 instaladas en el equipo es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio auxiliar de host para aplicaciones	AppHostSvc	Automático		
ASP.NET State Service	Aspnet_state	Automático		
Aplicación del sistema COM+	COMSysApp	Manual		
Servicio de administración IIS	IISADMIN	Automático		
Servicio de registro de W3C	w3logsvc	Automático		
Servicio de publicación World Wide Web	w3svc	Automático		
Servicio WAS	WAS	Automático		
Servicio de Administración Web	WMSVC	Manual		

Comprobación	OK/NOK	Cómo hacerlo
3. Verifique que se han asignado los permisos correctos en el sistema de archivos		Utilizando el Explorador de Windows: **"Windows+R → Explorer"** En caso de no saber dónde apunta cada una de las rutas abreviadas que se especifica, ejecute Explorer <<ruta>> donde <<ruta>> se sustituirá por la ruta abreviada. **Nota:** Para verificar los permisos de cada fichero o carpeta deberá abrir las propiedades del objeto, marcándolo con el botón derecho y eligiendo la opción "Propiedades" del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá situarse en la pestaña "Seguridad". En la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios. Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados.

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\System32\inetsrv\MetaBack	Administrador	Control total	
	System	Control total	
%SystemRoot%\System32\LogFiles	Administradores	Control Total	
	SYSTEM	Control Total	
	Creator Owner	Control Total	

4. Compruebe que el registro de acceso de IIS está operativo		En la configuración que ha realizado ha habilitado el registro de acceso al servidor, por lo que debe asegurarse que está registrando la actividad. Para ello verifique que el directorio **C:\inetpub\logs\W3SVC1** contiene ficheros con el formato **u_ex*fecha*.log**. Abriendo el último deberá ver que registra los accesos correctamente.  **Nota:** Tenga en cuenta que no se crea ningún registro hasta que no se realiza alguna actividad.

Comprobación	OK/NOK	Cómo hacerlo
5. Comprobación de la depuración de sistemas en producción		Compruebe que la depuración en sistemas de producción esta deshabilitada. Para ello chequee: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS) → [nombre_del_servidor] → Sitios → Editor de configuración → Sección: System.web/Compilation → Debug → False"**. 
6. Comprobación de las identidades del grupo de aplicaciones.		Compruebe que en las identidades del grupo de aplicaciones no hay identidades de servicio integradas. Para ello chequee: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS) → [nombre_del_servidor] → Grupo de aplicaciones"**. 

ANEXO A.3. CATEGORÍA MEDIA

ANEXO A.3.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 MIEMBROS DEL DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

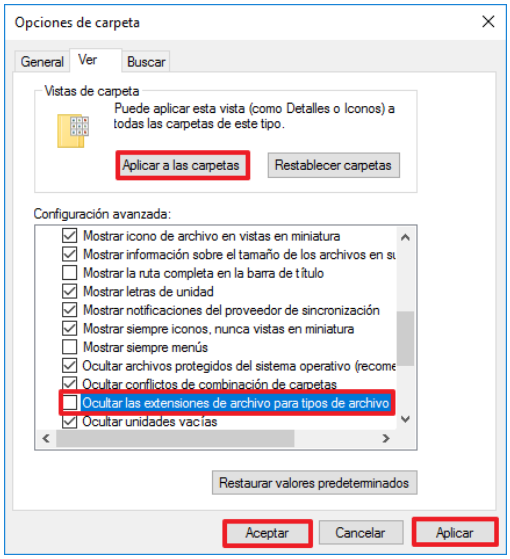
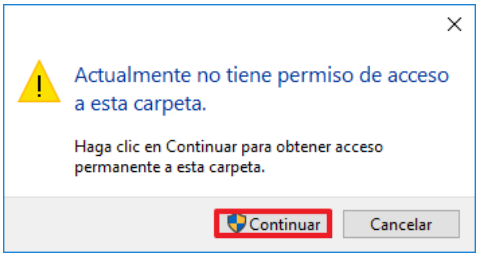
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tenga que securizar IIS 10 sobre Microsoft Windows Server 2016 con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran la categoría media, deberá realizar las implementaciones según se referencian en el presente anexo.

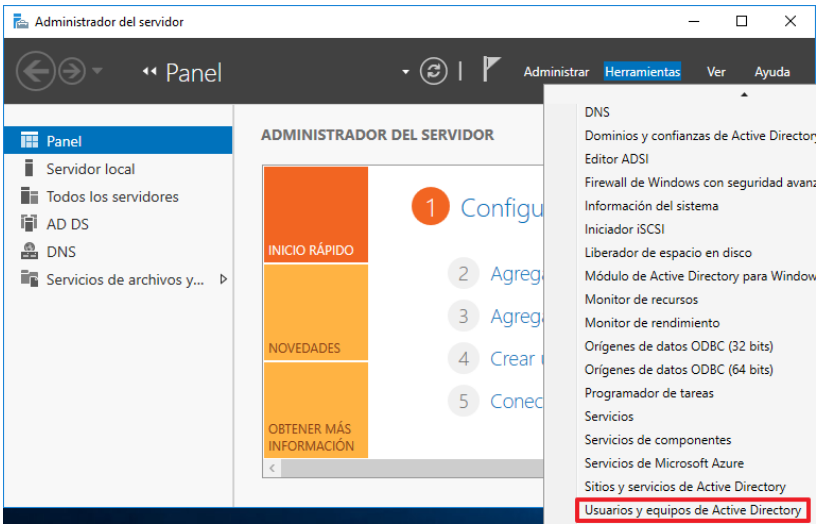
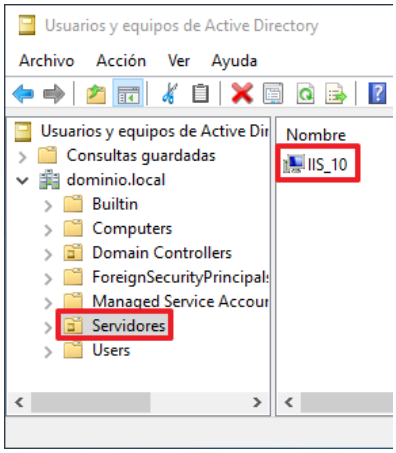
Debe tener en consideración que, antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

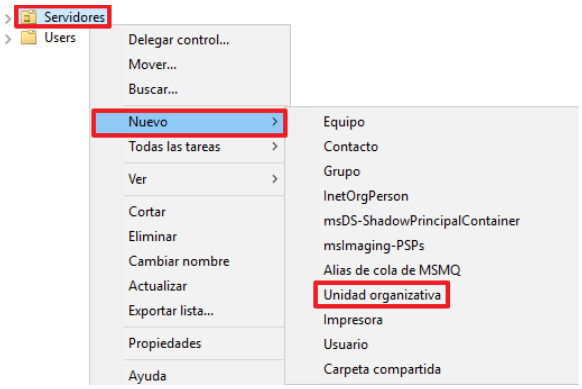
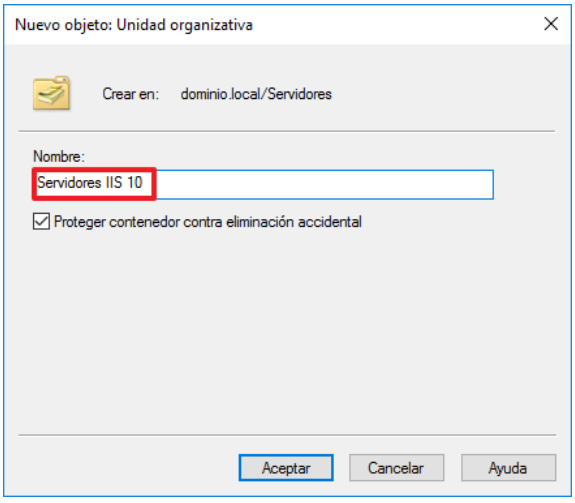
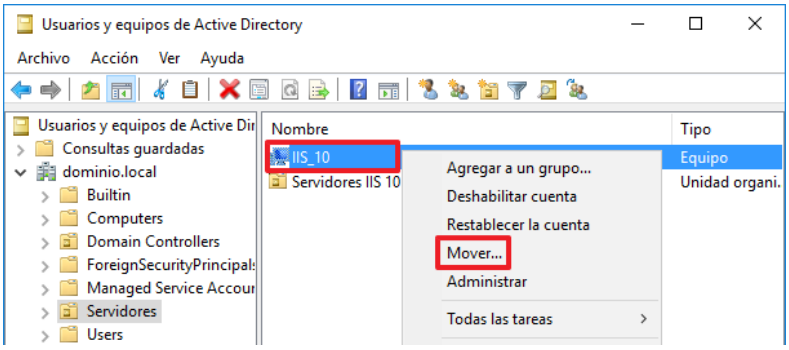
1. PREPARACIÓN DE DOMINIO

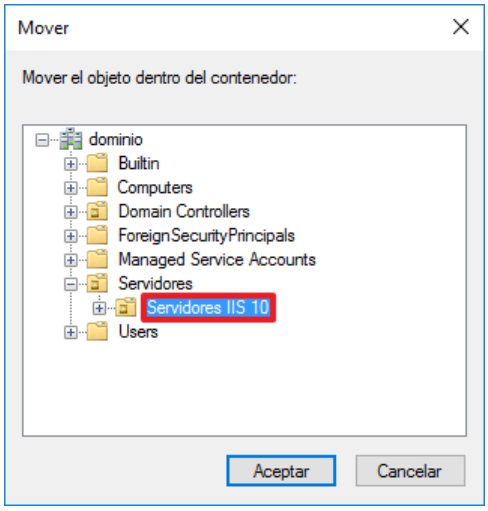
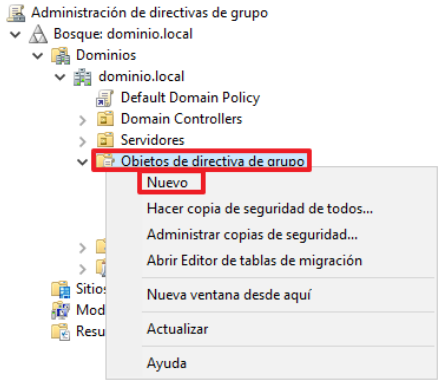
Los pasos que se describen a continuación se realizarán en un controlador de dominio del domino al que va a pertenecer el servidor Internet Information Services 10.

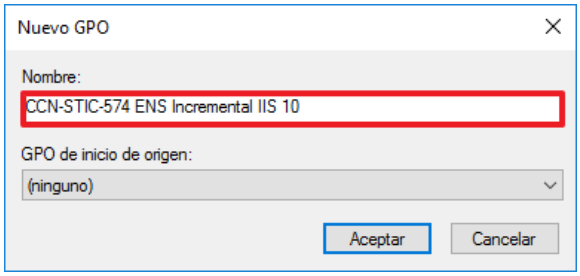
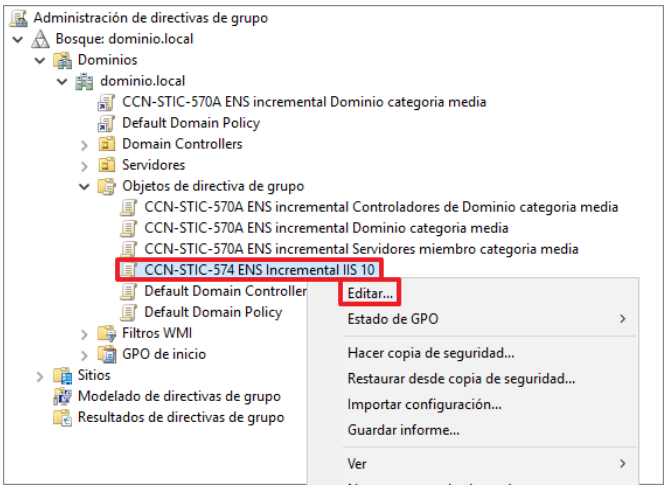
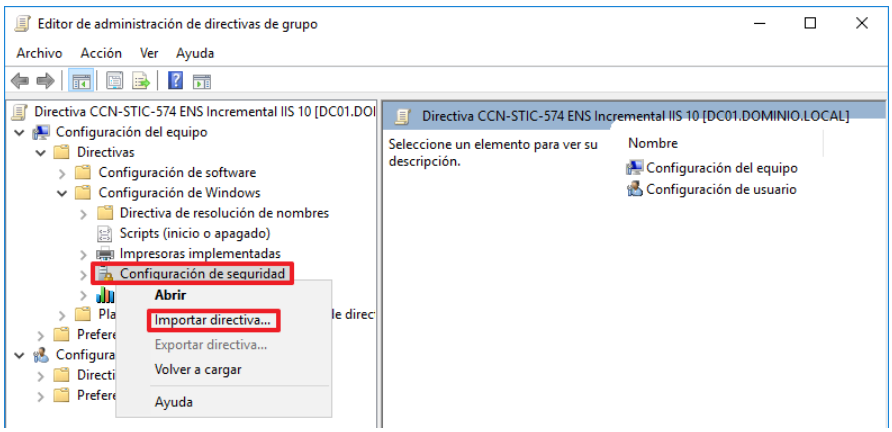
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.

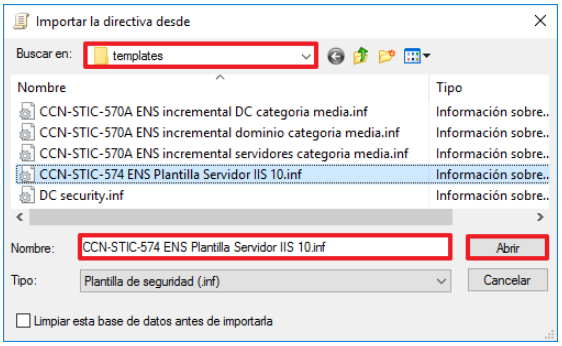
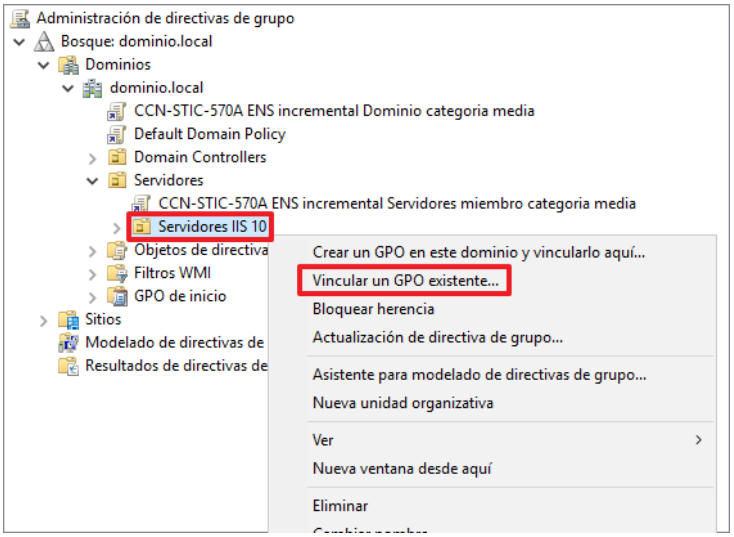
Paso	Descripción
4.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar “Explorador de Windows” y poder mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura:  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".
5.	Copie el fichero “CCN-STIC-574 ENS Plantilla Servidor IIS10.inf” al directorio “%SYSTEMROOT%\security\Templates” del controlador de dominio.  **Nota:** Según la configuración de seguridad de UAC, el sistema podría solicitar la elevación de privilegios por cada uno de ellos, en este caso, pulse “Continuar” en las 3 ocasiones que el sistema se lo solicita o marque la opción “Hacer esto para todos los elementos actuales” para pulsar “Continuar” en una sola ocasión.

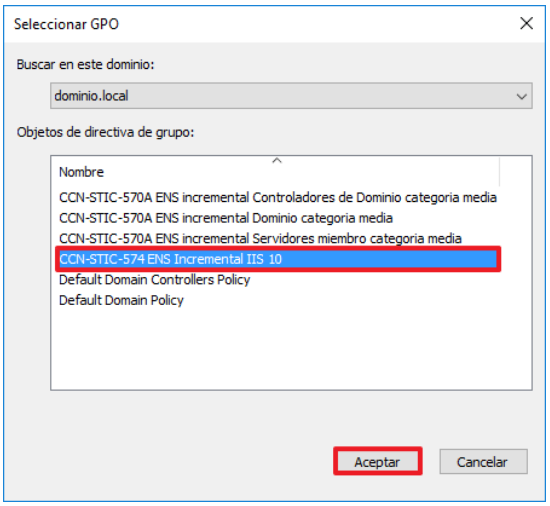
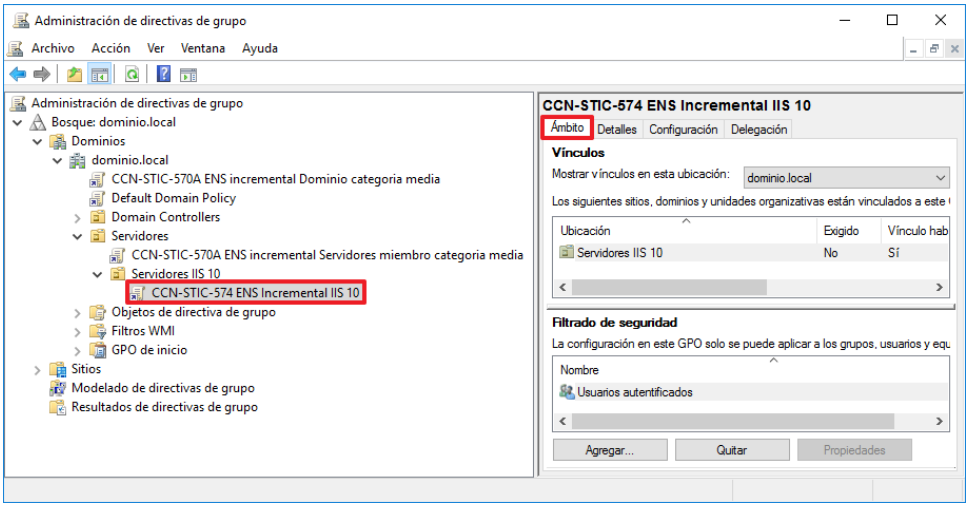
Paso	Descripción
6.	Inicie la herramienta de usuarios y equipos del Directorio Activo. Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione **"Herramientas → Usuarios y equipos de Active Directory"** 
7.	Despliegue el dominio y diríjase a la carpeta donde tiene alojados los servidores que tienen instalado el rol de IIS 10. **"Menú inicio→ Herramientas administrativas→ Usuarios y equipos de Active Directory→ [nombre del dominio]→ Servidores"**.  **Nota:** Si usted no desea crear unidades organizativas en su organización deberá adaptar estos pasos para alojar los servidores IIS 10 y vincular la GPO que se creará posteriormente a los servidores IIS 10 de su organización.

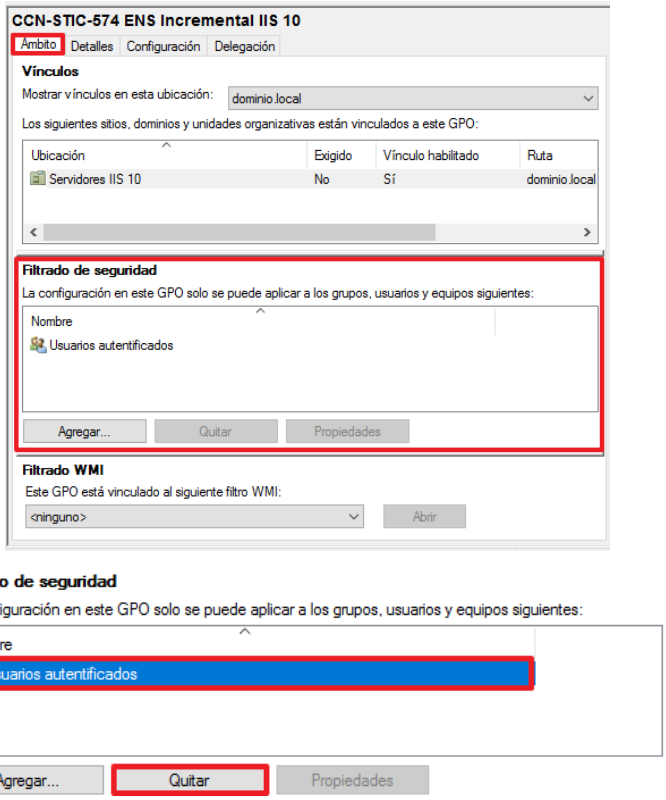
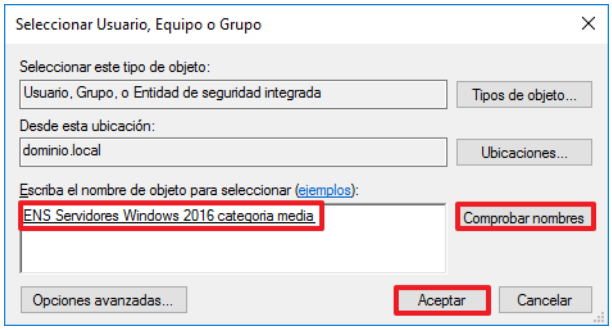
Paso	Descripción
8.	Solicite la creación de una nueva unidad organizativa utilizando el menú contextual, pulse botón derecho sobre la unidad organizativa “Servidores” y despliegue **“Nuevo → Unidad organizativa”**. 
9.	En la consola, cree una unidad organizativa denominada “Servidores IIS 10” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen. 
10.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores IIS 10 a la unidad organizativa “Servidores IIS 10”. Para ello, deberá hacer clic botón derecho sobre “Mover…” en el servidor que desee ubicar en la nueva unidad organizativa. 

Paso	Descripción
11.	A continuación, seleccionamos la unidad organizativa “Servidores IIS 10”. 
12.	Cierre la herramienta de “Usuarios y equipos de Directorio Activo”
13.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administración de directivas de grupo”** 
14.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”.
15.	Pulse con el botón derecho, sobre dicha y carpeta y seleccione la opción “Nuevo”. 

Paso	Descripción
16.	Introduzca como nombre “CCN-STIC-574 ENS Incremental IIS 10” y pulse el botón “Aceptar”. 
17.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
18.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**
19.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva…”. 

Paso	Descripción
20.	Seleccione de la ruta "C:\Windows\security\templates" el fichero "CCN-STIC-574 Plantilla Servidor IIS 10" y pulse el botón "Abrir". 
21.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
22.	A continuación, seleccione la unidad organizativa "Servidores IIS 10" y pulse botón derecho, "Vincular un GPO existente". 

Paso	Descripción
23.	Seleccione el objeto de directiva de grupo con nombre, “CCN-STIC-574 ENS Incremental IIS 10” y pulse aceptar. 
24.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
25.	Seleccione la nueva política de grupo configurada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 

Paso	Descripción
26.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
27.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación.
28.	Una vez quitado, pulse el botón “Agregar…”.
29.	Introduzca como nombre “ENS servidores Windows 2016 categoria media”. Este grupo corresponde con el generado en la aplicación de la guía CCN-STIC-570A. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.

2. CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

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

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

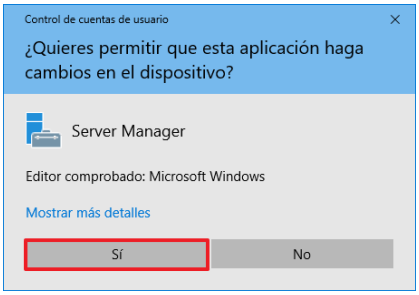
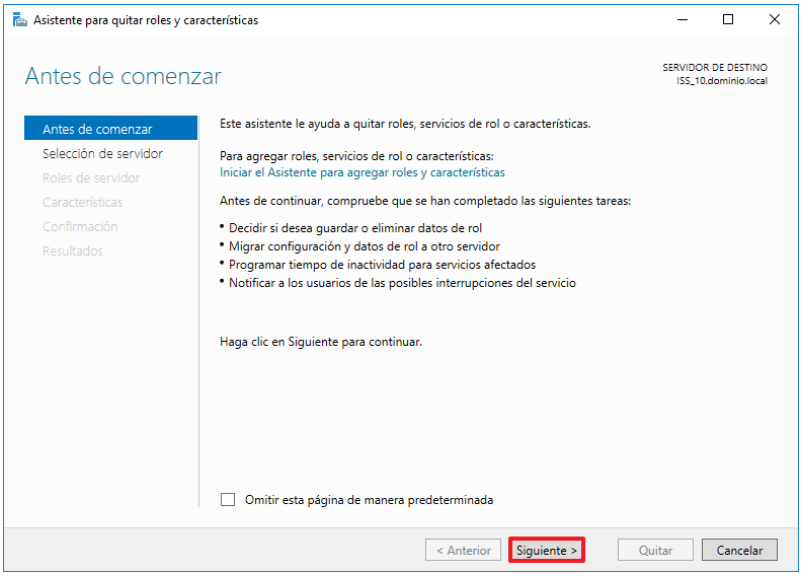
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

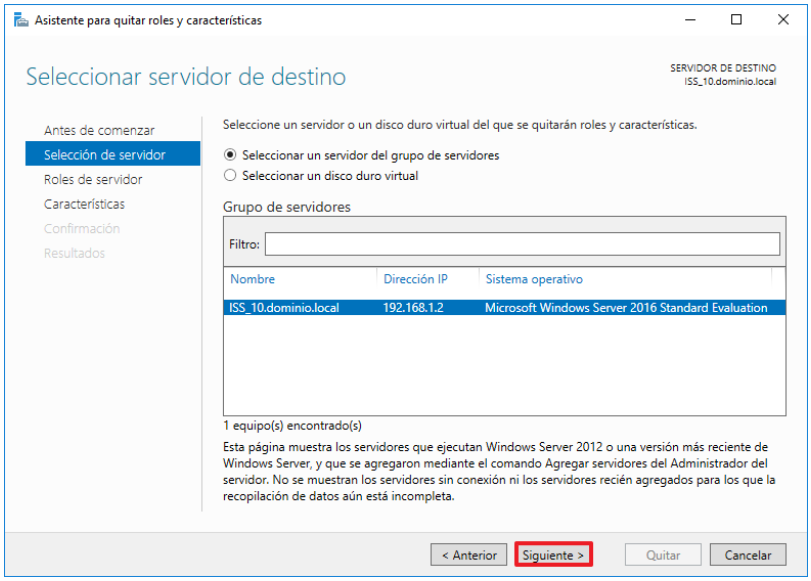
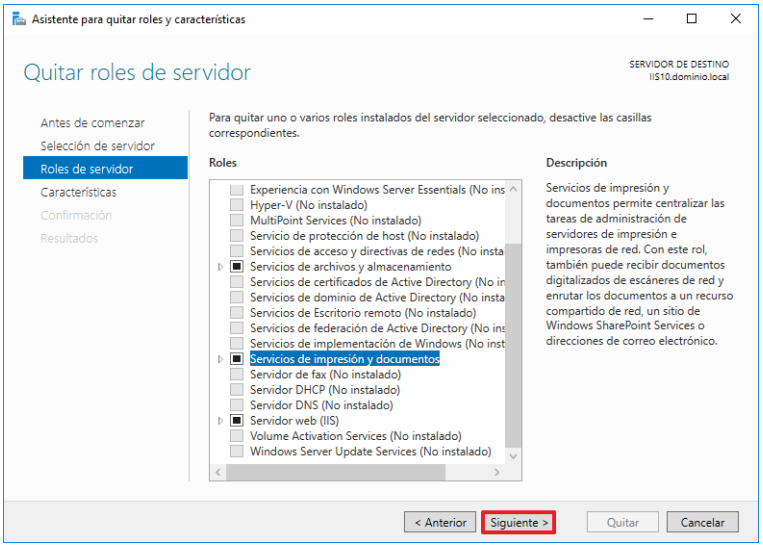
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

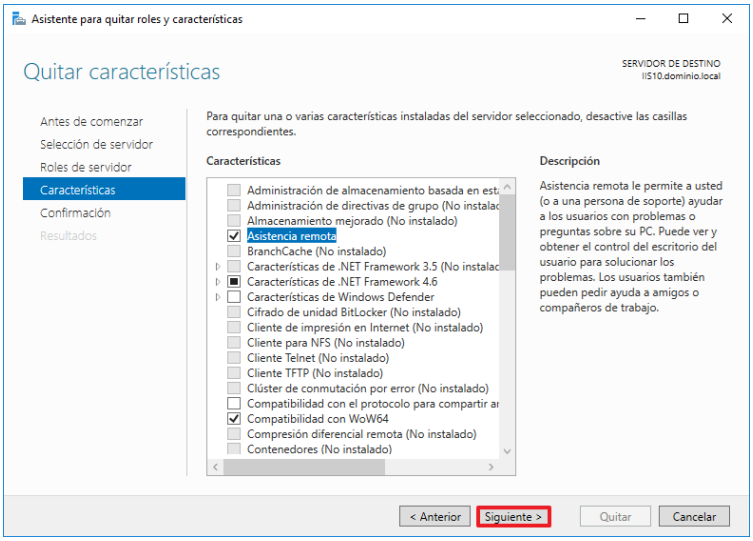
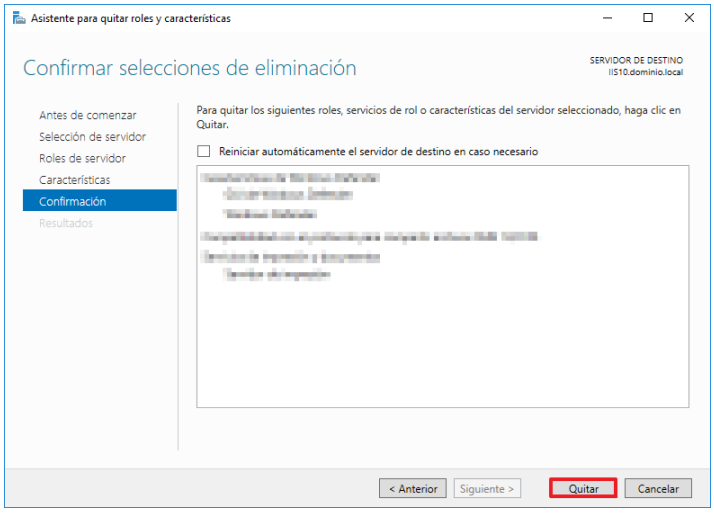
Es recomendable que el sitio web este alojado en otra ubicación de disco diferente a la del sistema operativo y que esta solo se utilice para el alojamiento de sitios web, evitando con ello exponer más información de la estrictamente necesaria.

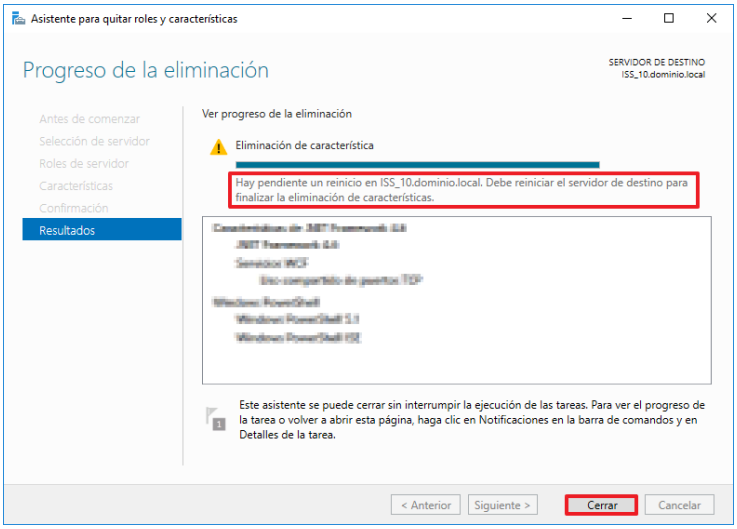
Para realizar el siguiente paso a paso deberá realizar previamente el paso “3.1 PREPARACIÓN DEL DIRECTORIO ACTIVO” y una vez finalizado deberá realizar el paso “3.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

Paso	Descripción
30.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado el rol de IIS 10. 
31.	Pulse sobre el administrador del servidor. 

Paso	Descripción
32.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar. 
33.	A continuación, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Administrar → Quitar roles y funciones”**. 
34.	Comenzará el asistente para quitar roles y características, pulse sobre el botón “Siguiente >”. 

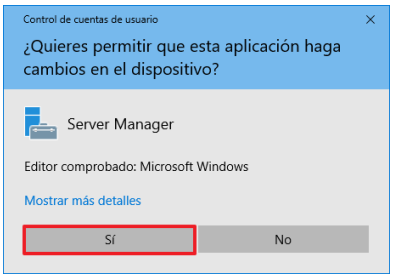
Paso	Descripción
35.	Seleccione el servidor donde desea quitar las características del IIS 10 y pulse siguiente. 
36.	En la siguiente ventana podrá quitar roles del servidor, en este caso pulse siguiente para acceder a las características de los roles instalados. 

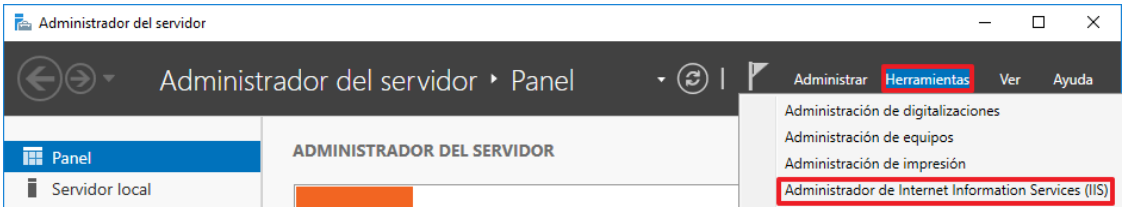
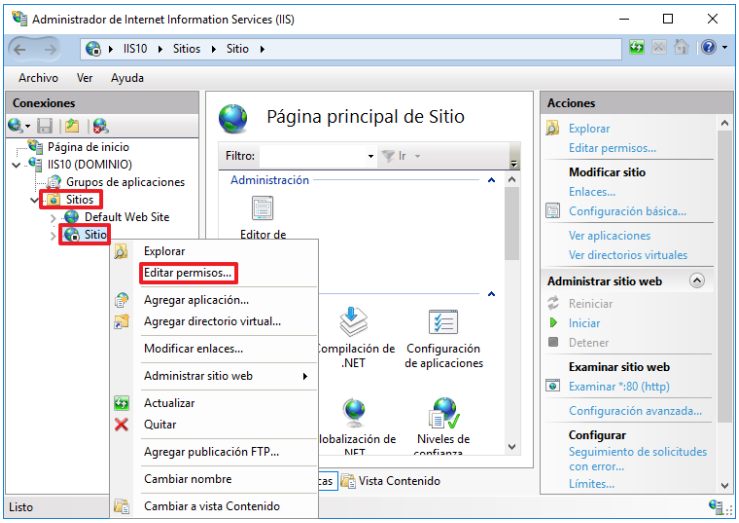
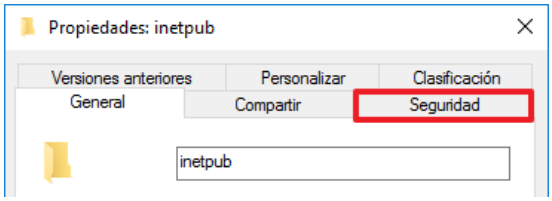
Paso	Descripción
37.	A continuación, seleccione las características que desea quitar. 
38.	La siguiente pantalla mostrara las características a modos resumen que desea quitar, confirme que las características seleccionadas son las correctas y pulse “Quitar”. 

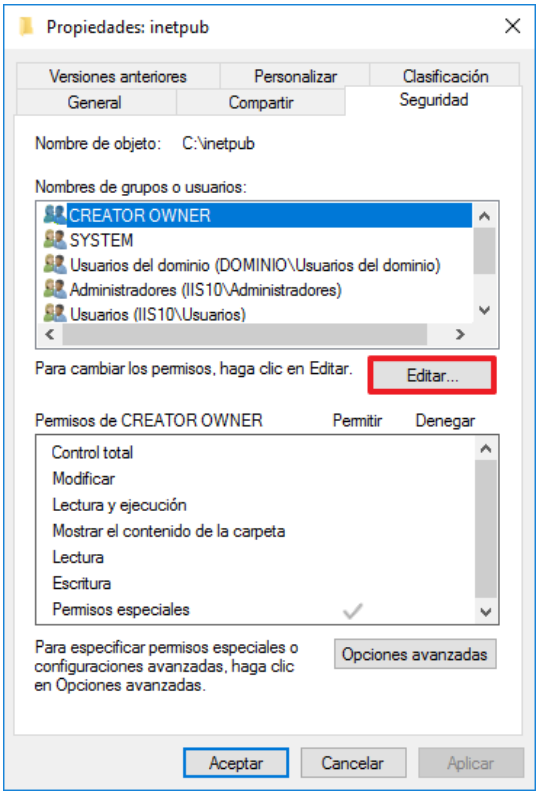
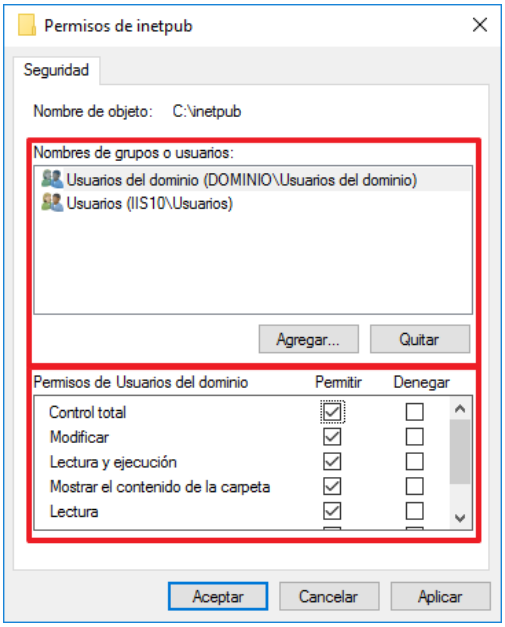
Paso	Descripción
39.	Una vez finalizada la desinstalación pulse “Cerrar”.  **Nota:** Debe tener en cuenta que la desinstalación de determinadas características puede requerir el reinicio del equipo.

2.2. GESTION DE PERMISOS RECURSOS WEB

En este apartado se tendrá en consideración la gestión y administración del acceso a los recursos web según el marco operacional de categoría media establecido por el ENS, para con ello limitar y controlar el acceso a directorios con información sensible de ser sustraída.

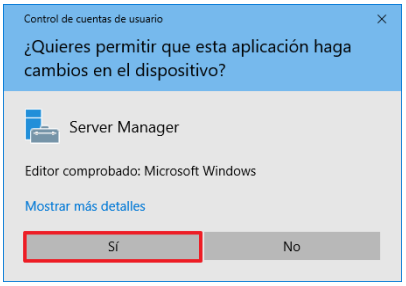
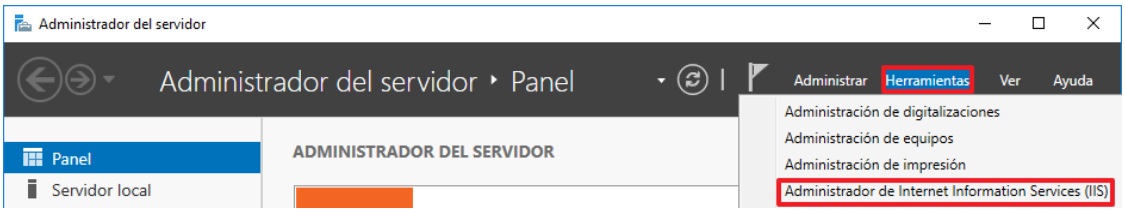
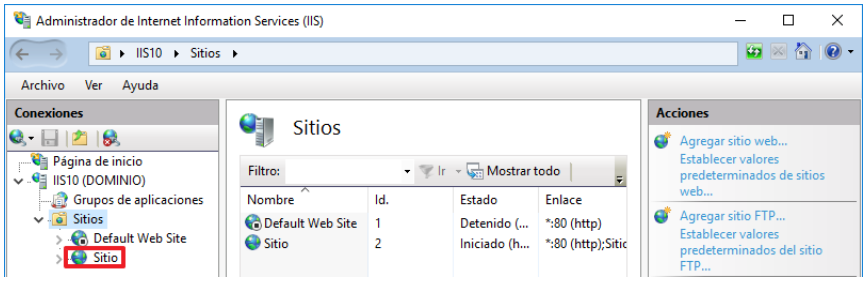
Paso	Descripción
40.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
41.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 

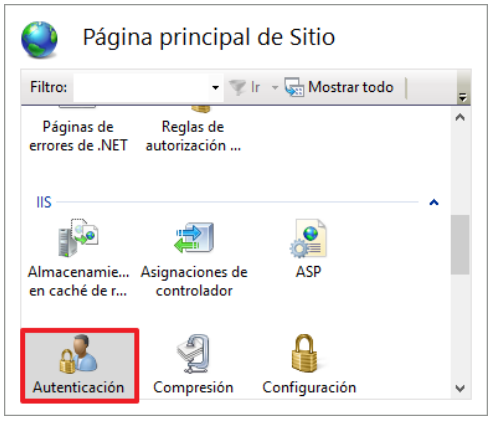
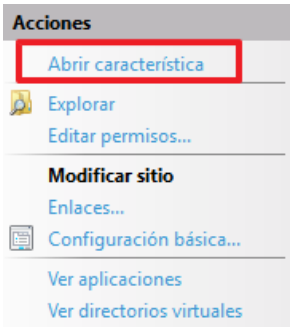
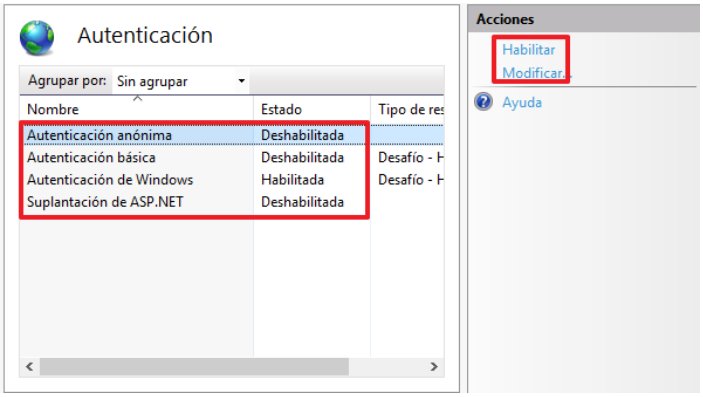
Paso	Descripción
42.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”** 
43.	Pulse botón derecho sobre el sitio al cual quiere asignar o quitar permisos. 
44.	Diríjase hasta la pestaña “Seguridad”. 

Paso	Descripción
45.	A continuación, pulse el botón “Editar”. 
46.	A continuación, seleccione los permisos del que desea establecer para ese sitio web.  **Nota:** Es recomendable dar permiso solo a los usuarios o grupos que deban tener acceso al sitio web evitando que el usuario administrador tenga permiso para prevenir posibles vulnerabilidades.

2.3. AUTENTICACIÓN SITIO WEB

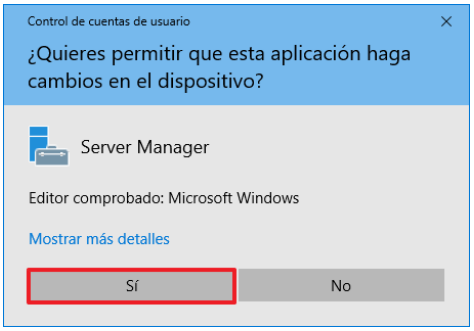
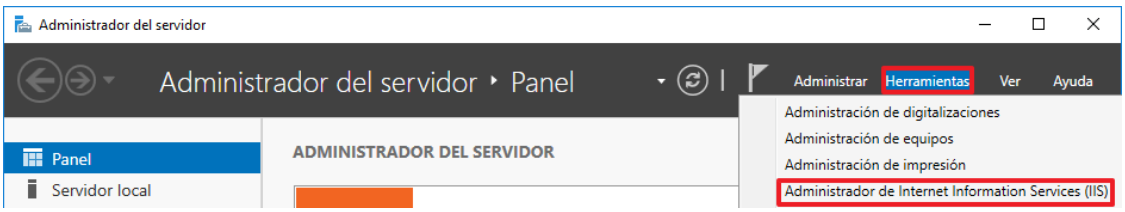
Los métodos de autenticación permitirán limitar el acceso al sitio web a una lista determinada de usuarios (el método habilitado por defecto de los servicios web de IIS es la autenticación anónima), en todas las categorías de seguridad se debe limitar el acceso al contenido web a usuarios anónimos para prevenir posibles ataques.

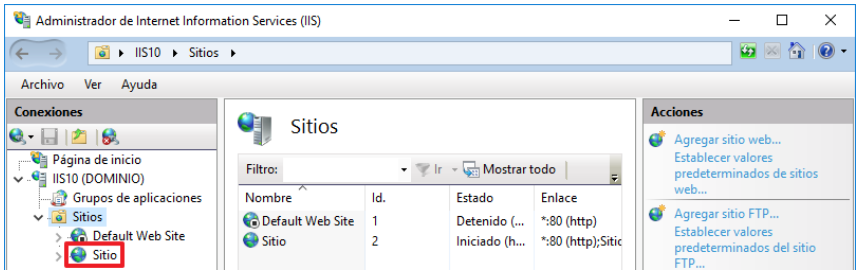
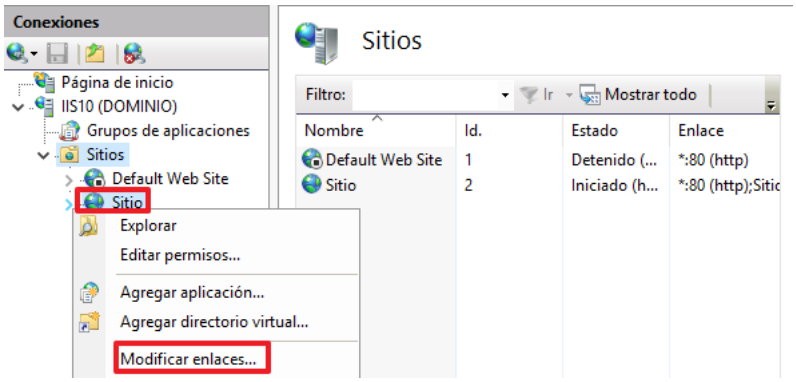
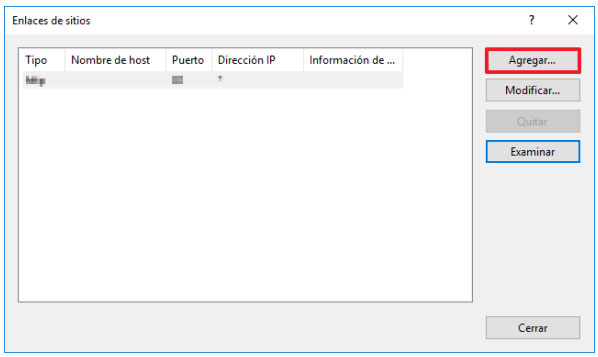
Paso	Descripción
47.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
48.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar. 
49.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”** 
50.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo de “*Conexiones*” y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.

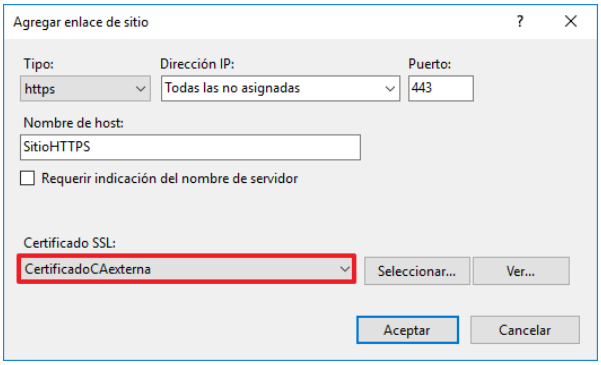
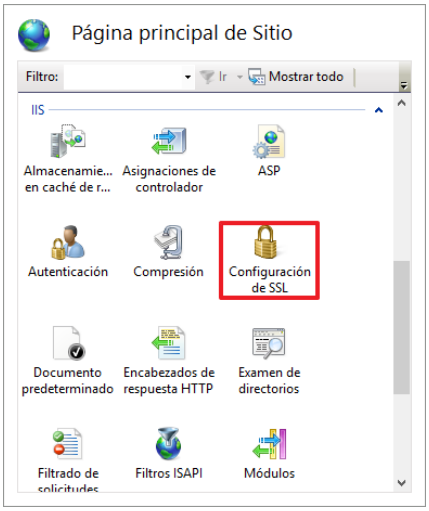
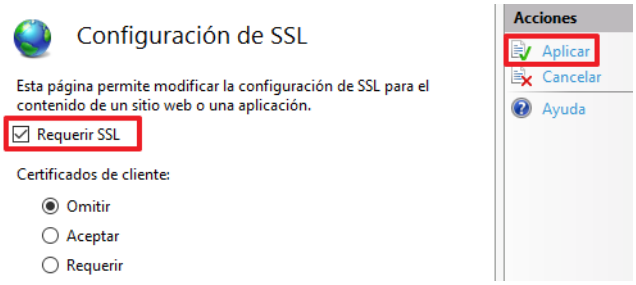
Paso	Descripción
51.	Seleccione en la página principal del sitio web el icono de “Autenticación”. 
52.	Pulse sobre “Abrir característica” situado en el panel derecho en el menú “Acciones”. 
53.	A continuación, establezca según las características de su organización los métodos de autenticación disponibles. Para ello pulse sobre el método de autenticación que quiere configurar y en el panel derecho seleccione la acción que desea realizar.  **Nota:** Únicamente se usará la autenticación anónima para páginas webs generales en la que solo se muestre contenido y no sea necesaria la autenticación del usuario.

2.4. CERTIFICADOS

IIS 10 faculta el empleo de protocolos seguros para las comunicaciones y los procesos de autenticación usando HTTPS que utiliza un cifrado basado en SSL/TLS para crear un canal cifrado para el tráfico de información sensible. Para lugares públicos es un requisito indispensable en la categoría media del ENS el uso de certificados emitidos por entidades certificadoras de terceros reconocidas, para el caso de sitios internos se recomienda el uso de certificados emitidos por una entidad certificadora interna, está totalmente desaconsejado el uso de certificados autofirmados.

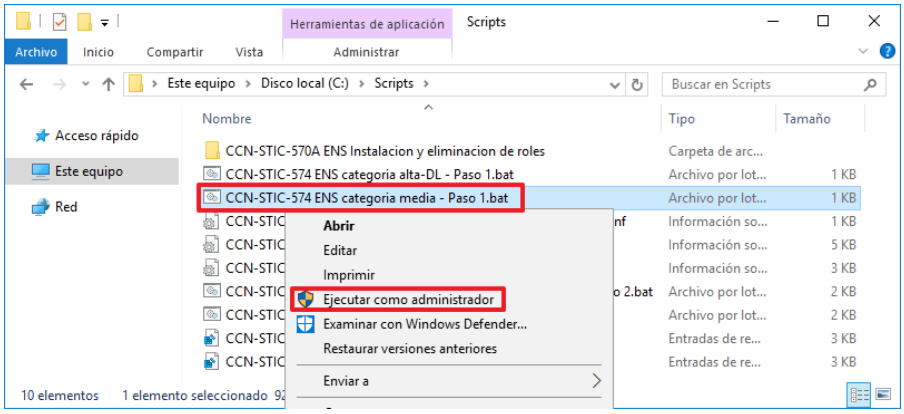
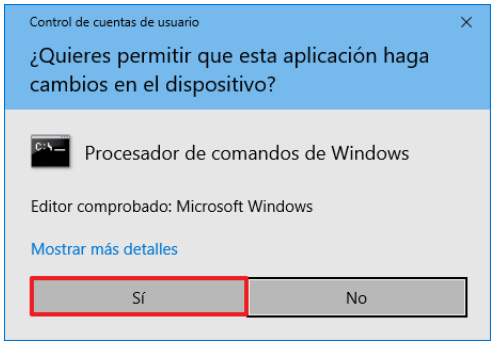
Paso	Descripción
54.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
55.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 
56.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”** 

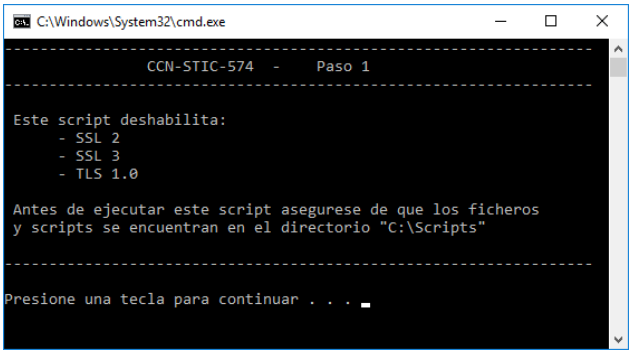
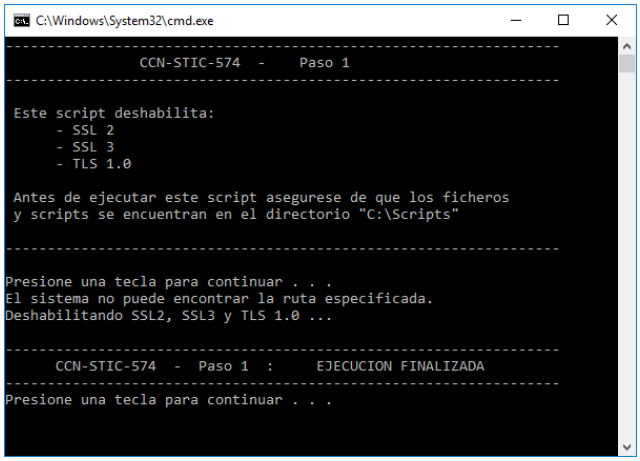
Paso	Descripción
57.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo de "*Conexiones*" y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.
58.	Pulse con el botón derecho sobre el sitio web que quiere modificar y seleccione la opción "Modificar enlaces…". 
59.	Pulse sobre el botón "Agregar…". 

Paso	Descripción
60.	Seleccione Tipo: “Https” y a continuación seleccione el Certificado SSL de una entidad externa y pulse “Aceptar”. 
61.	A continuación, deberá configurar el sitio web para que los usuarios requieran un certificado propio, para ello pulse sobre en el sitio web que desea configurar, y seleccione “Configuración de SSL”: 
62.	Seleccione la opción de “Requerir SSL” y pulse sobre “Aplicar” para que el sistema guarde los cambios realizados. 
63.	En caso de que usted no cuente con un certificado emitido por una entidad certificadora autorizada debe solicitarlo para cumplir con la categoría media de seguridad del ENS.

2.5. PROTOCOLOS DE TRANSMISIÓN

Con la aplicación del ENS para la categoría media sobre IIS 10 es imprescindible eliminar el uso de los algoritmos SSL2, SSL3 y TLS1.0, evitando con ello sufrir posibles ataques.

Paso	Descripción
64.	Inicie sesión en el servidor miembro donde tiene instalado el rol de IIS 10.
65.	Si no lo ha realizado anteriormente, cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
66.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.
67.	A continuación, debe ejecutar el *script* 1 para deshabilitar los protocolos anteriormente indicados, es necesario realizar esta acción con elevación de privilegios, debe hacer clic con el botón derecho, sobre el fichero denominado “CCN-STIC-574 ENS categoria media – Paso 1.bat” situado en “C:\Scripts” y haga clic en “Ejecutar como administrador”. 
68.	El control de cuentas de usuario le solicitará elevación de permisos para ejecutar el programa, pulse “Si”. 

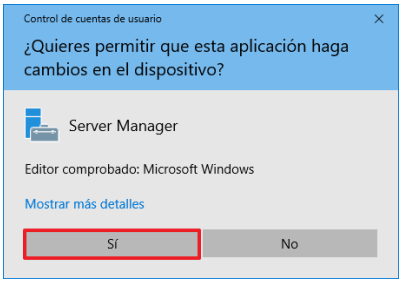
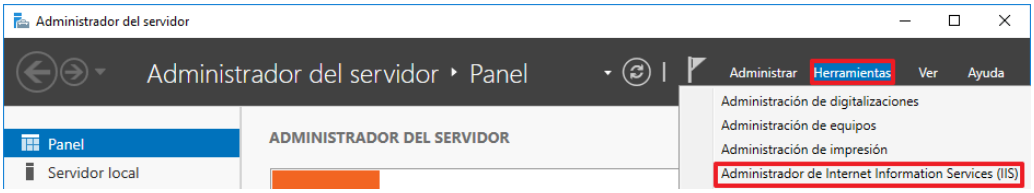
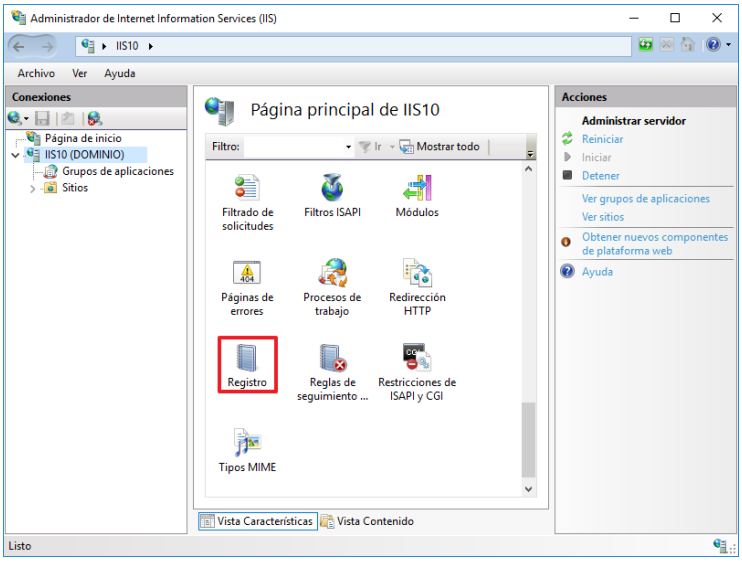
Paso	Descripción
69.	Aparecerá la siguiente ventana indicando que va a proceder a deshabilitar los protocolos SSL2, SSL3 y TLS 1.0, pulse cualquier tecla para continuar. 
70.	Una vez finalizada la tarea pulse una tecla para cerrar la ventana. 

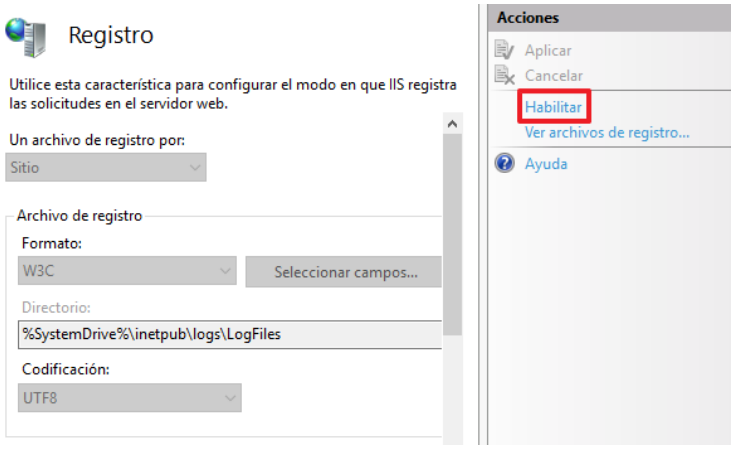
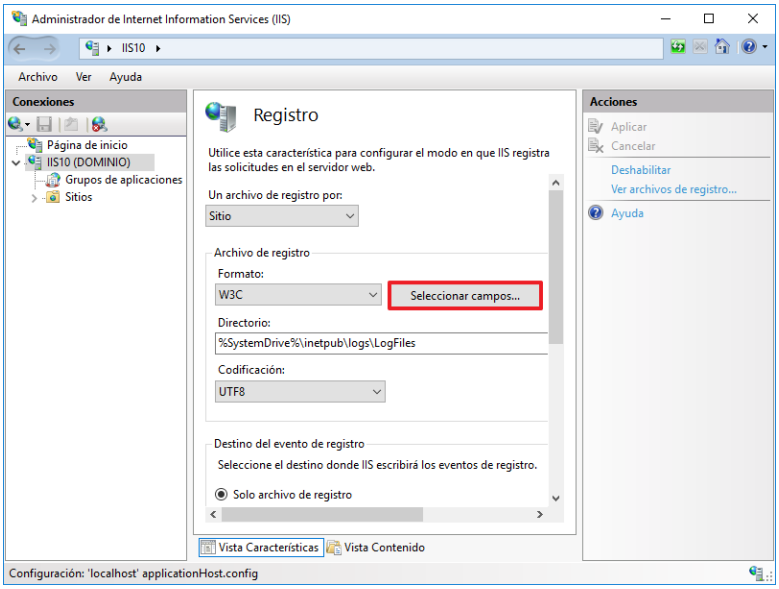
2.6. AUDITORÍA

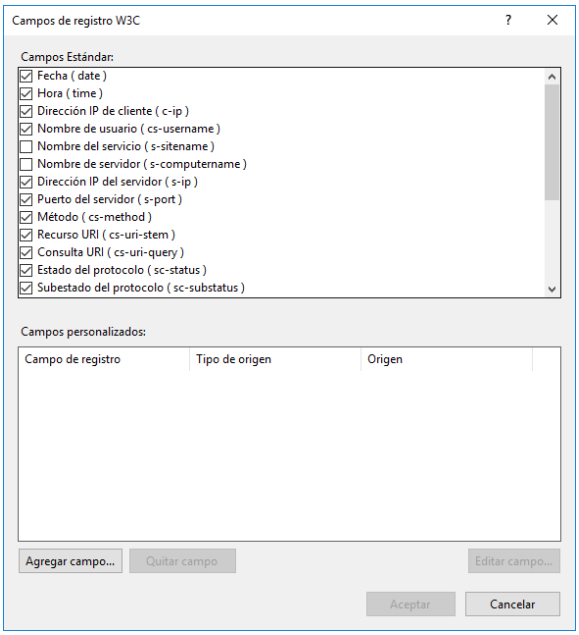
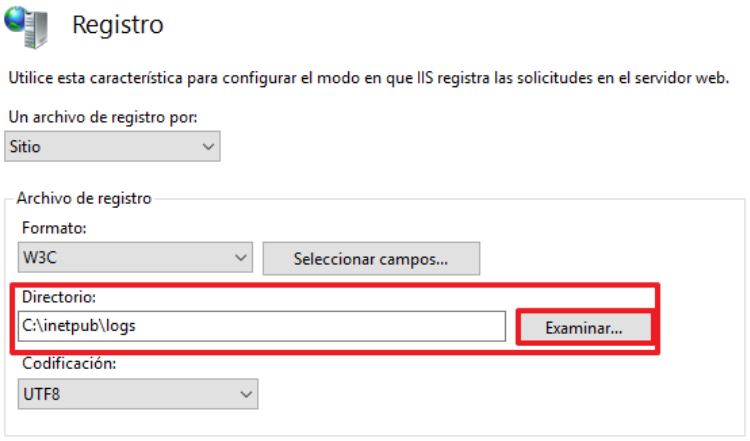
Con la aplicación del ENS para la categoría media sobre IIS 10 quedará registrado el uso del sistema para poder detectar y reaccionar a cualquier fallo accidental o deliberado, quedando registrado en el sistema quien realiza la actividad, cuando y sobre qué información con el fin de detectar anomalías o intentos frustrados de acceso a información no autorizada.

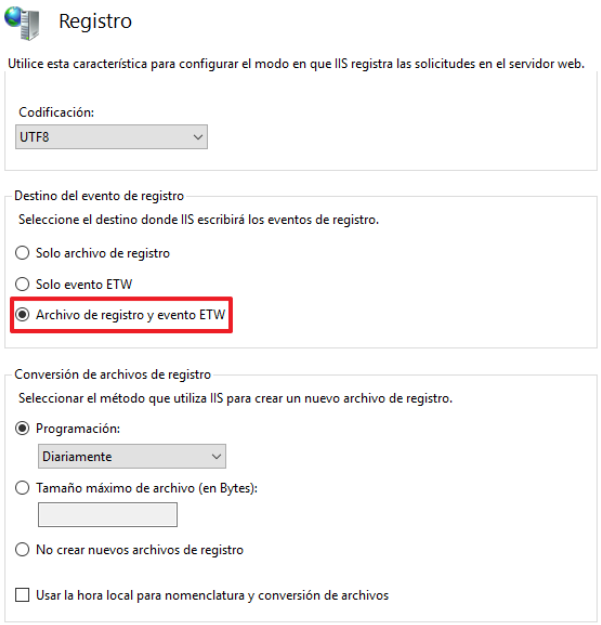
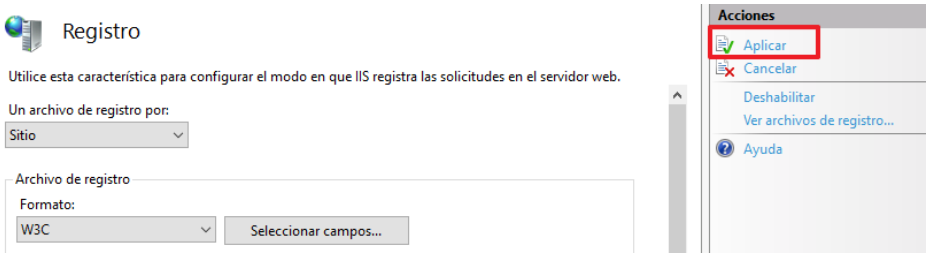
La ubicación de los registros debe ser diferente a la del sistema además de tener limitado el acceso únicamente a los usuarios autorizados.

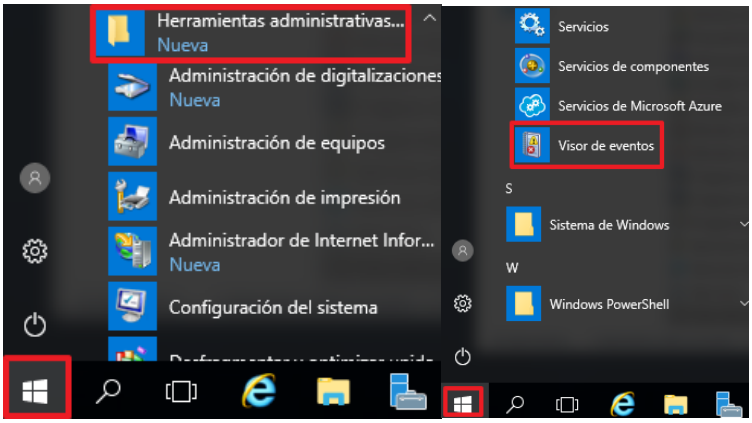
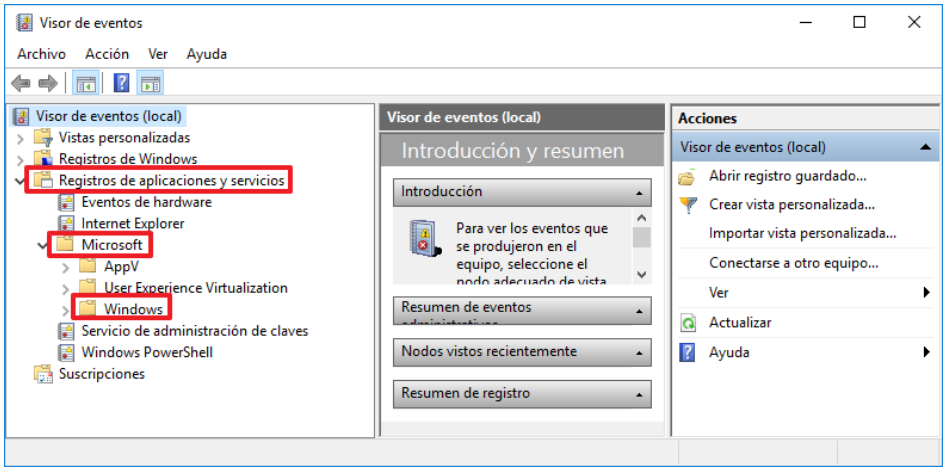
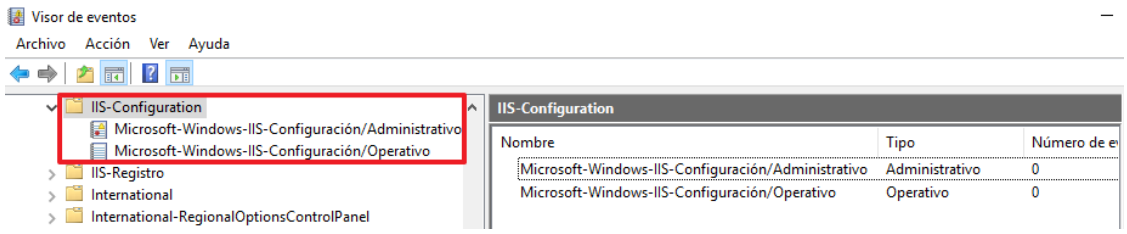
Paso	Descripción
71.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 

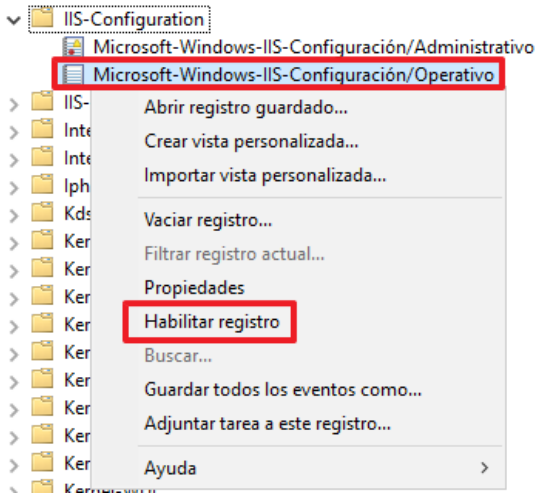
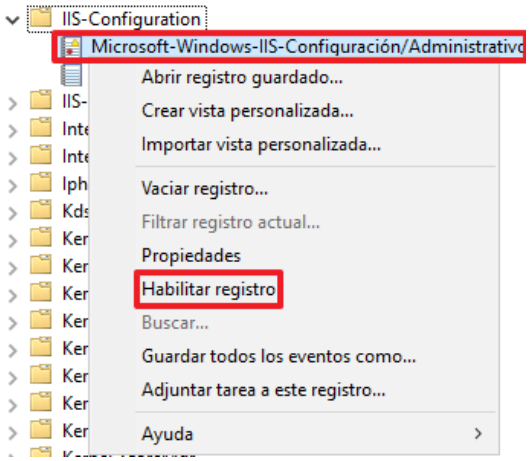
Paso	Descripción
72.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar. 
73.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”** 
74.	Diríjase al sitio web que desea administrar, a continuación, localice el icono “Registro”, y pulse la acción “Abrir característica” situado en la parte superior derecha de la pantalla para acceder a la configuración del registro. 

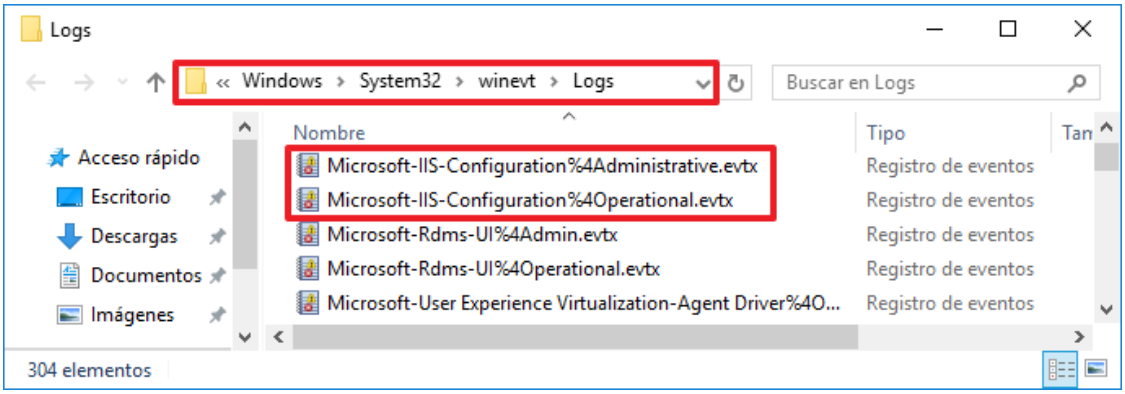
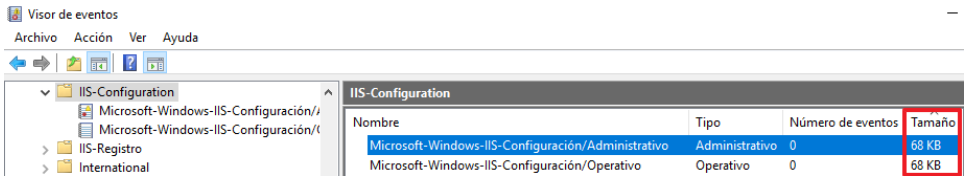
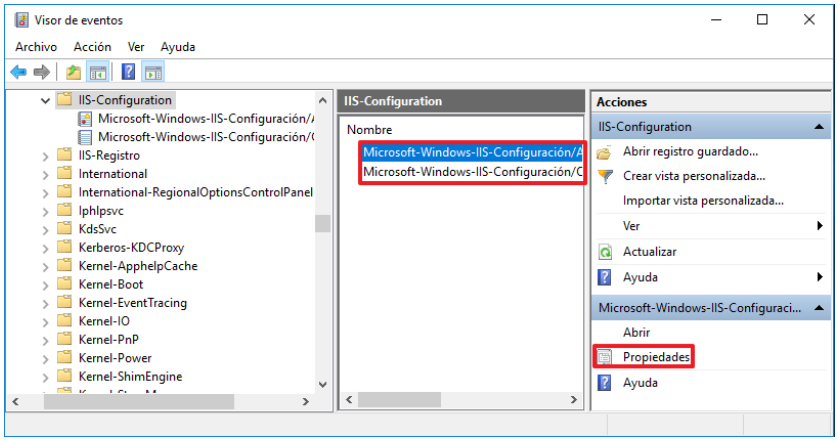
Paso	Descripción
75.	Debe habilitar el registro de las solicitudes del servidor IIS 10 para ello, diríjase al menú "Acciones" situado en la parte superior derecha de la pantalla y pulse sobre "Habilitar". 
76.	Seleccione los campos que desea registrar, para ello pulse sobre "Seleccionar campos…". 

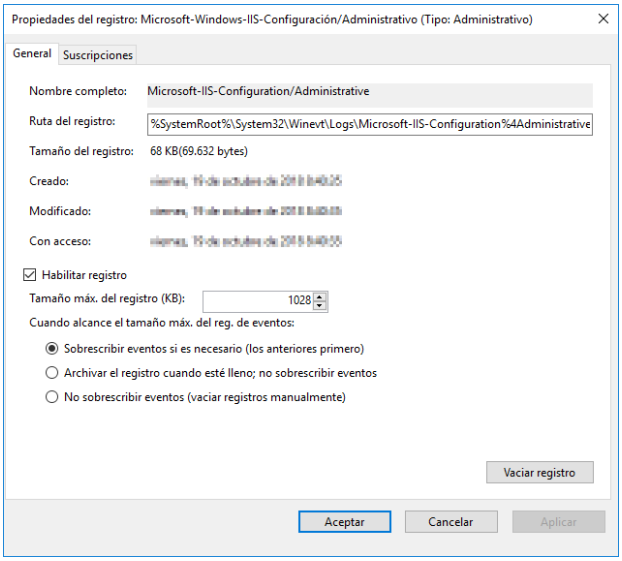
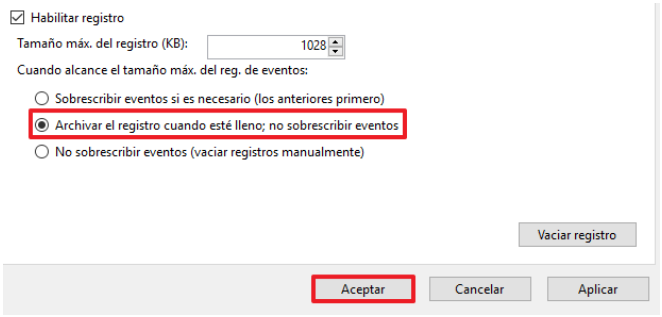
Paso	Descripción
77.	Compruebe qué campos se recogerán en el fichero de registro y asegúrese que coincide con sus necesidades. Los valores marcados por defecto suelen ser suficientes, pero no descarte marcar otros. 
78.	A continuación, seleccione el directorio donde se van a guardar los registros, por seguridad es recomendable realizarlo en una unidad diferente a la de la instalación del sistema operativo. 

Paso	Descripción
79.	A continuación, deberá seleccionar el destino del evento, seleccione, “Archivo de registro y evento ETW”. 
80.	Una vez realizados los cambios deberá guardarlos, para ello pulse “Aplicar” situado en el menú “Acciones” en la parte superior izquierda de la pantalla. 
81.	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.

Paso	Descripción
82.	Debe abrir el Visor de eventos, ejecutándolo como administrador, como en ocasiones anteriores. "**Menú inicio → Herramientas administrativas → Visor de eventos**".  **Nota:** El sistema solicitará elevación de privilegios para completar la acción.
83.	Seleccione en el árbol "**Visor de eventos → Registro de aplicaciones y servicios → Microsoft → Windows**". 
84.	Desplácese hacia abajo, podrá observar que Microsoft Windows Server 2016 dispone de dos grupos de registros para IIS, dentro del de configuración se encuentran: administrativo y operaciones. Es necesario activar ambos, según se le indica a continuación. 

Paso	Descripción
85.	Sitúese sobre el registro operativo, abra el menú contextual con el botón derecho del ratón y seleccione “Habilitar registro”.  **Nota:** Cualquier acción operativa sobre el servidor quedará recogida a partir de ahora.
86.	Haga lo mismo para el registro “Administrativo”. 

Paso	Descripción
87.	Los registros se habrán creado en el disco duro, en la partición del sistema operativo (habitualmente la C:) y en la ruta **%SystemRoot%\System32\winevt\Logs**, con los nombres: Microsoft IIS-Configuration%4Operational.evtx y Microsoft IIS-Configuration%4Administrative.evtx  **Nota:** La variable %SystemRoot% corresponde a C:\Windows en las configuraciones habituales de las guías.
88.	Los ficheros se crean con tamaño cero pero se empezarán a poblar automáticamente desde este momento: 
89.	Para acceder a las propiedades de los ficheros, seleccione un fichero y pulse sobre la opción “Propiedades” del menú “Acciones”.  **Nota:** Tenga en cuenta que el registro administrativo se llenará, en condiciones normales, antes que el operacional.

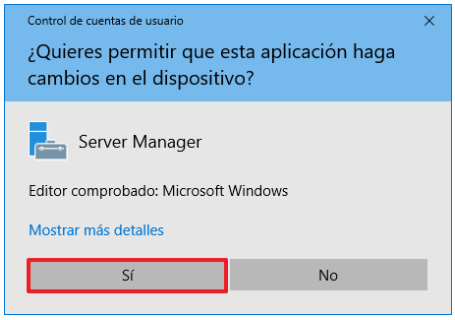
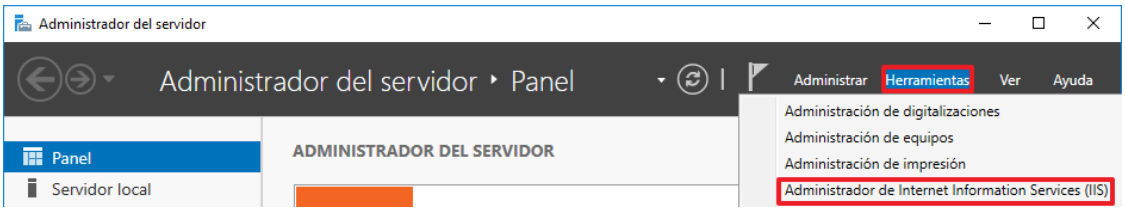
Paso	Descripción
90.	La siguiente pantalla muestra la configuración, propiedades, por defecto.  **Nota:** Tenga en cuenta que el registro administrativo se llenará, en condiciones normales, antes que el operacional.
91.	Para evitar, que una vez completado el fichero de registro, se empiece a borrar por 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".
92.	Con la configuración dejada, 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". Y el fichero de auditoría se vacía y comienza a llenarse de nuevo. **Nota:** Estos ficheros deberán ser copiados y eliminados periódicamente para evitar su pérdida y el llenado del disco duro.

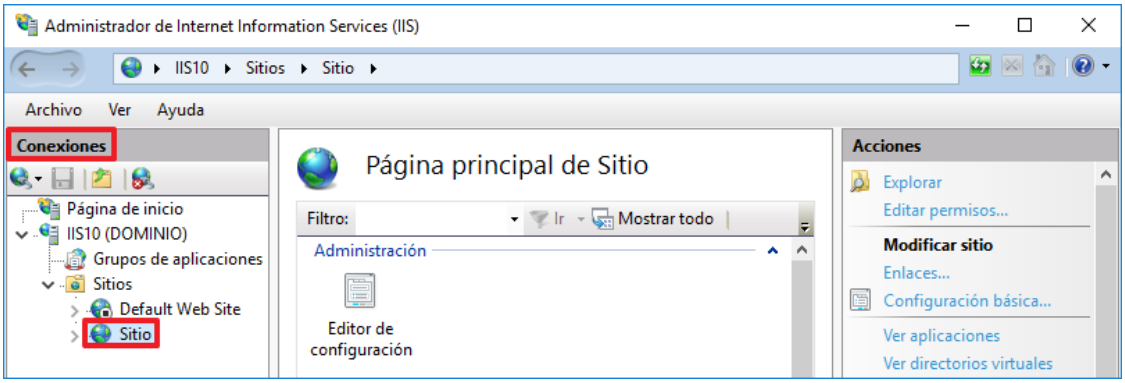
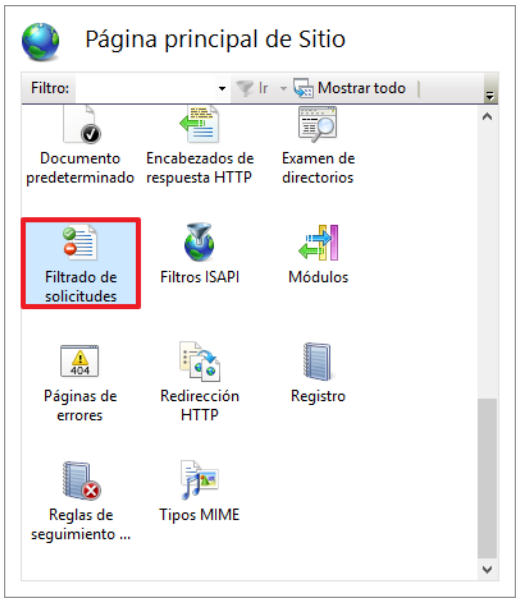
2.7. FILTRADO DE SOLICITUDES

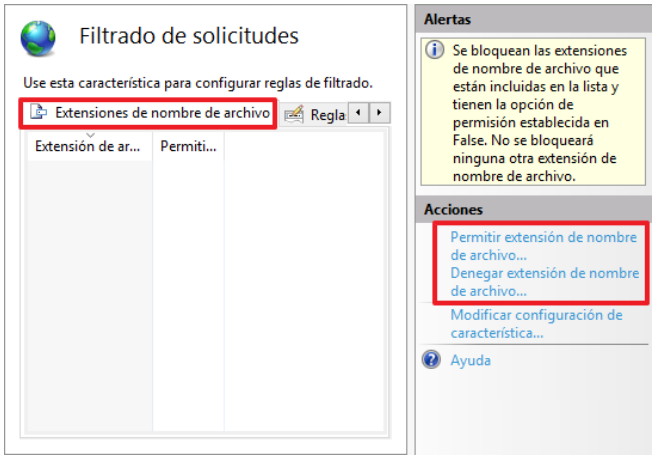
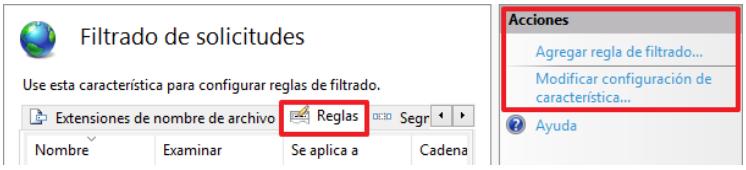
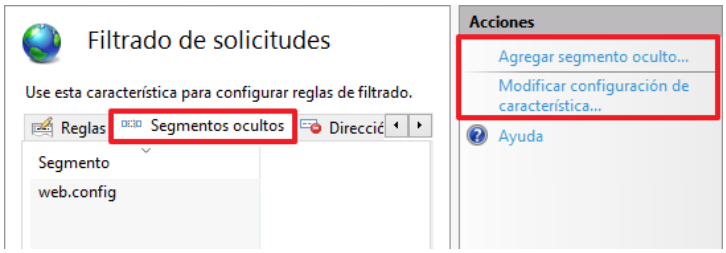
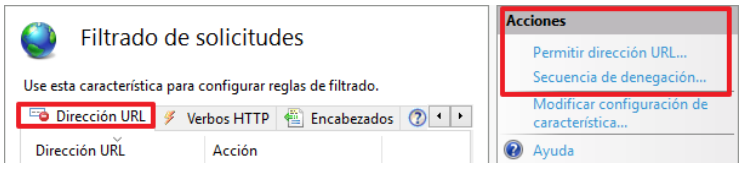
El siguiente paso define el procedimiento para la configuración del filtro de solicitudes el cual se encarga de analizar todas las solicitudes que entran en el servidor web y las filtra basándose en reglas establecidas previamente.

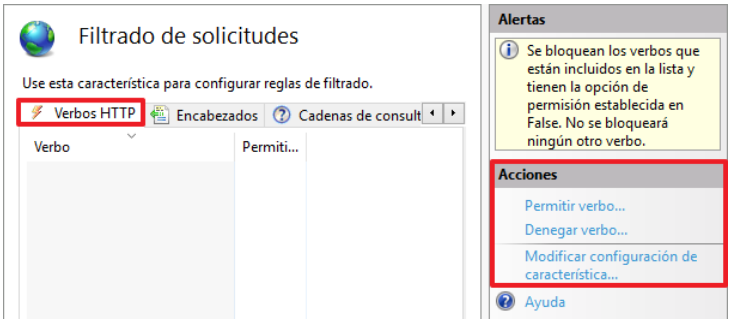
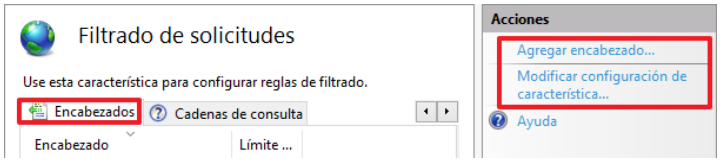
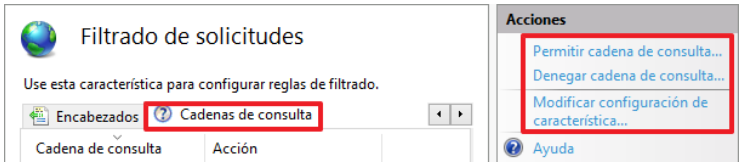
La mayoría de los ataques malintencionados comparten características comunes, como direcciones URL muy largas o solicitudes de una acción inusual, es por ello que filtrando las solicitudes se puede reducir el impacto de este tipo de ataques.

Cada organización debe determinar que extensiones son las específicamente necesarias para la funcionalidad del sitio web que tiene alojado y deberá configurar el filtro para soportar únicamente las extensiones exclusivamente necesarias.

Paso	Descripción
93.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
94.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 
95.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”** 

Paso	Descripción
96.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo de "*Conexiones*" y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.
97.	Seleccione en la página principal del sitio web el icono "Filtrado de solicitudes" y pulse sobre "Abrir característica" sitiado en el menú acciones del panel superior derecho de la pantalla. 

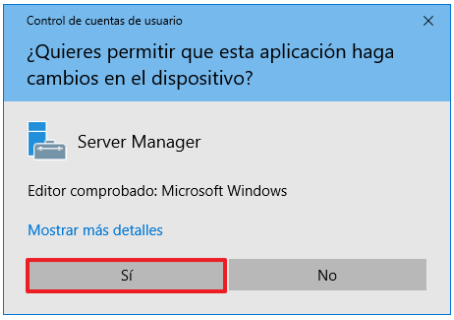
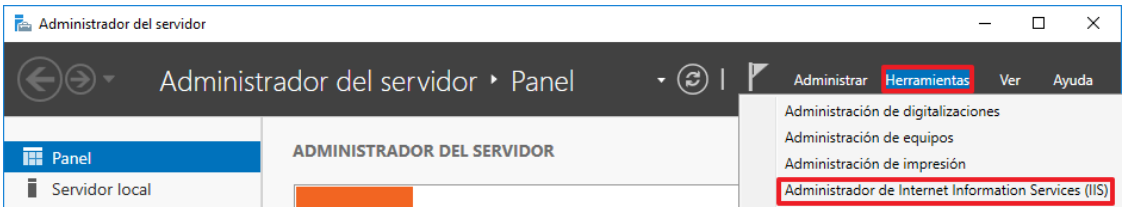
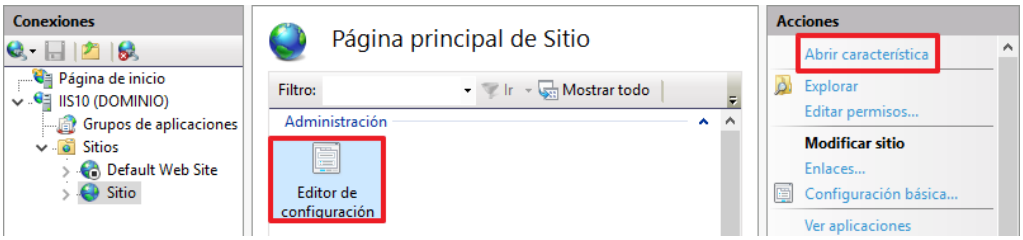
Paso	Descripción
98.	A continuación, en la pestaña “Extensiones de nombre de archivo” puede permitir o denegar extensiones. 
99.	En la siguiente pestaña puede agregar o modificar reglas de filtrado. 
100.	En la siguiente pestaña puede agregar o modificar segmentos ocultos. 
101.	En la siguiente pestaña puede permitir, denegar o modificar direcciones URL. 

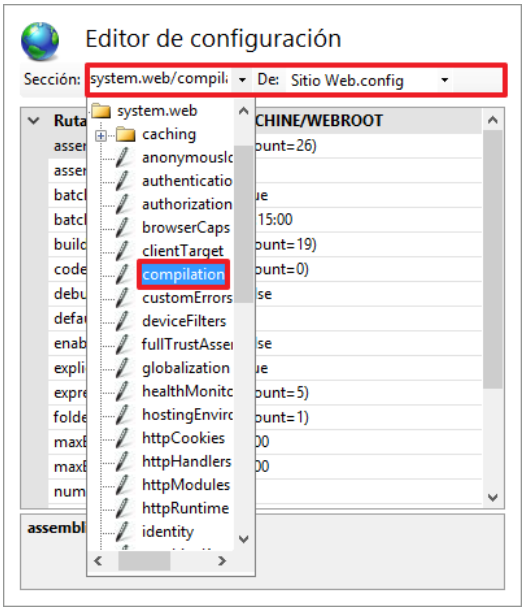
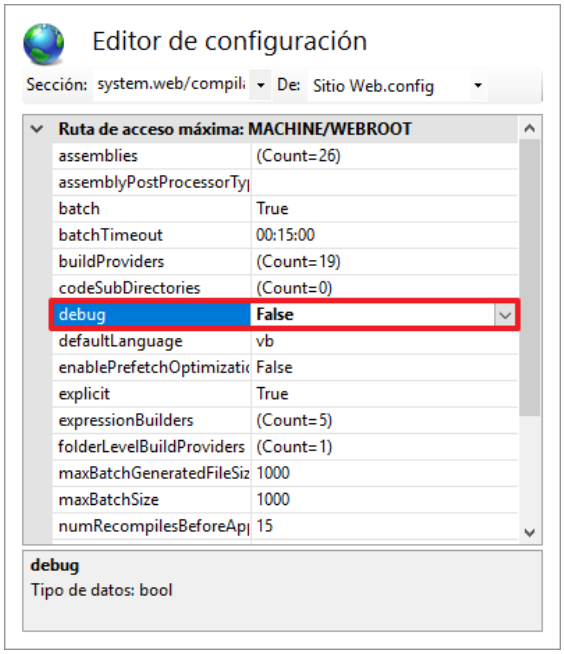
Paso	Descripción
102.	En la siguiente pestaña puede permitir, denegar o modificar Verbos. 
103.	En la siguiente pestaña puede agregar o modificar encabezados. 
104.	En la siguiente pestaña puede permitir, denegar o modificar cadenas de consulta. 

2.8. DESHABILITAR MODOS DE DEPURACIÓN

El siguiente paso define el procedimiento para la modificación del fichero web.config para inhabilitar el modo de depuración de una aplicación en entornos de producción, evitando con ello posibles fisuras de seguridad.

Paso	Descripción
105.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 

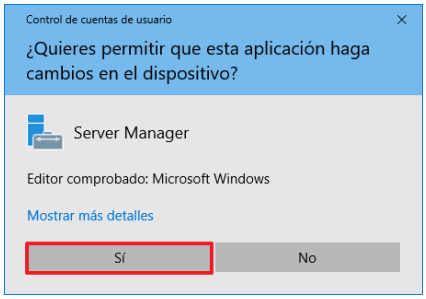
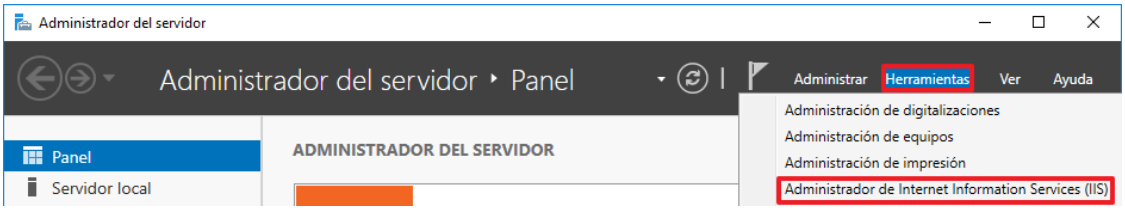
Paso	Descripción
106.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar. 
107.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”**. 
108.	Localice el sitio web que desea configurar y seleccione “Editor de configuración”, a continuación, pulse en el menú “Acciones” la opción “Abrir característica” situado en la parte superior derecha de la pantalla para abrir el editor de configuración. 

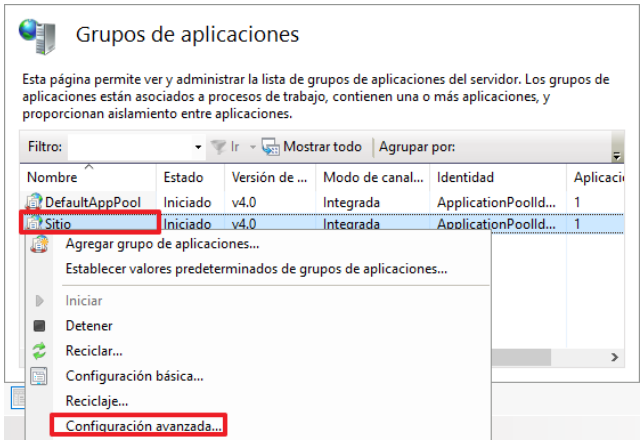
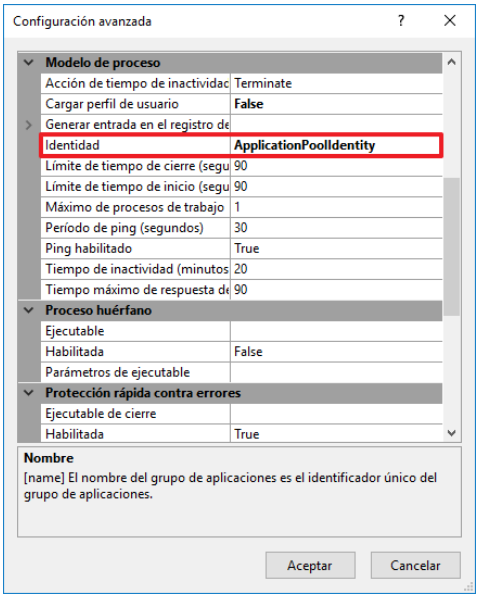
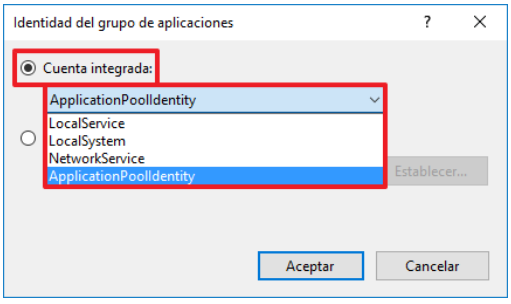
Paso	Descripción
109.	Navegue en “Sección” hasta “system.web/compilation”. 
110.	Localice la opción “Debug”, abra el desplegable y seleccione “False”. 

2.9. IDENTIDADES DEL GRUPO DE APLICACIONES

El siguiente paso define el procedimiento para la modificación de las identidades de una aplicación las cuales deben modificarse con la aplicación del ENS para la categoría media sobre IIS 10 y evitando el uso de identidades de servicio integradas tales como servicio local o sistema local.

Para una mayor seguridad los grupos de aplicaciones deben ejecutarse bajo la identidad del grupo cuando se crea el grupo de aplicaciones, el valor predeterminado y más seguro es "ApplicationPoolIdentity". El uso de una cuenta personalizada es aceptable, pero debe asegurarse de usar una cuenta diferente para cada grupo de aplicaciones.

Paso	Descripción
111.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
112.	El sistema solicitará elevación de privilegios. Pulse sobre el botón "Sí" para confirmar. 
113.	Inicie la herramienta "Administrador de Internet Information Services (IIS)". Para ello, pulse sobre el menú superior de la derecha de la herramienta "Administrador del servidor" y seleccione **"Herramientas → Administrador de Internet Information Services (IIS)"** 
114.	Despliegue el servidor y seleccione la opción "Grupos de aplicaciones". 

Paso	Descripción
115.	A continuación, seleccione la aplicación que desea configurar y haga clic botón derecho sobre ella y pulse “Configuración avanzada…”. 
116.	Localice la opción “Identidad” dentro de “Modelo de proceso”. 
117.	A continuación, seleccione la opción que más se adecue a sus necesidades y pulse “Aceptar”. 

2.10. LIMPIEZA DE METADATOS

Se ha de tener en consideración que en un servidor web se pueden alojar documentos que pueden contener información oculta en los metadatos los cuales contienen información que permite catalogar, ordenar y clasificar nuestros archivos, por lo que pueden ser un riesgo de seguridad para nuestra organización, por lo que hay que tener especial atención en la limpieza de los metadatos de los documentos que se alojan en el servidor web por ello antes de alojar un fichero en el servidor web se ha debido de realizar el procedimiento indicado en MP. INFO. 6. LIMPIEZA DE DOCUMENTOS**.**

En el proceso de limpieza se ha de tener en consideración que se retiraran todos los datos de los documentos además de la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, con la excepción de la información pertinente para el receptor del documento.

2.11. SOLUCIONES WAF (WEB APLICATION FIREWALL)

Un servidor web puede alojar aplicaciones por lo que es importante un control exhaustivo de estas por ello se han de emplear uno de los elementos principales en la protección de entornos de aplicaciones Web que son los cortafuegos (firewalls) de aplicaciones Web, también conocidos como WAF, Web Application Firewall.

El WAF se encargará de proteger los servidores de aplicaciones web de determinados ataques específicos en Internet además de controlar las transacciones al servidor web de nuestra organización.

Este sistema nos permite evitar probables ataques como:

a) “Cross-site scripting” que consiste en la inclusión de código script malicioso en el cliente que consulta el servidor web.

b) “SQL injection” que consiste en introducir un código SQL que vulnere la Base de Datos de nuestro servidor.

c) “Denial-of-service” que consiste en que el servidor de aplicación sea incapaz de servir peticiones correctas de usuarios.

Algunos sistemas WAF existentes en el mercado también monitorizan las respuestas del servidor, por ejemplo, si en una respuesta, que el servidor web envía al usuario se detectan cadenas que pueden ser identificadas como cuentas bancarias, el WAF lo puede detectar como un posible ataque y denegar la respuesta.

3. GESTIÓN DE ROLES Y/O CARACTERÍSTICAS DEL SISTEMA

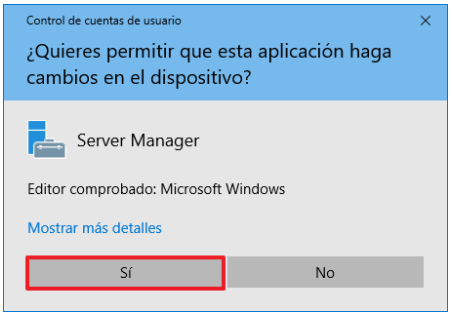
Estos paso a paso se deberán aplicar para instalar o desinstalar roles y/o características implementadas en un servidor miembro del dominio, que le sea de aplicación la guía de securización “CCN-STIC-570A - Implementación del ENS en Microsoft Windows Server 2016” a partir de la categoría media del ENS.

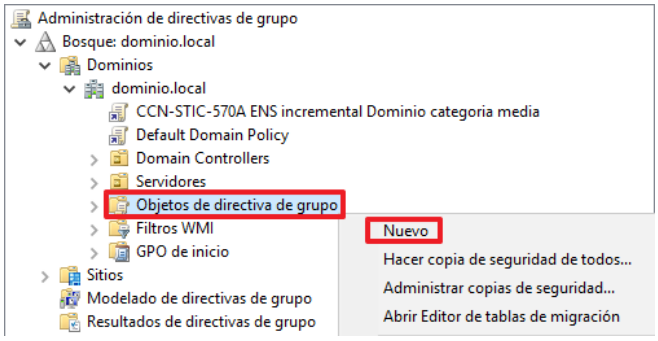
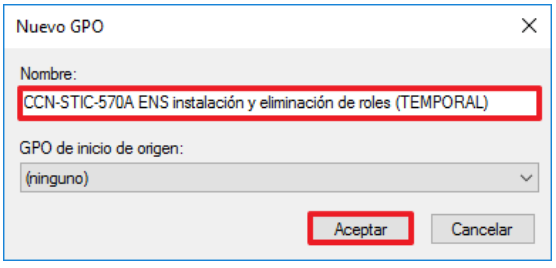
3.1. PREPARACIÓN DEL DIRECTORIO ACTIVO

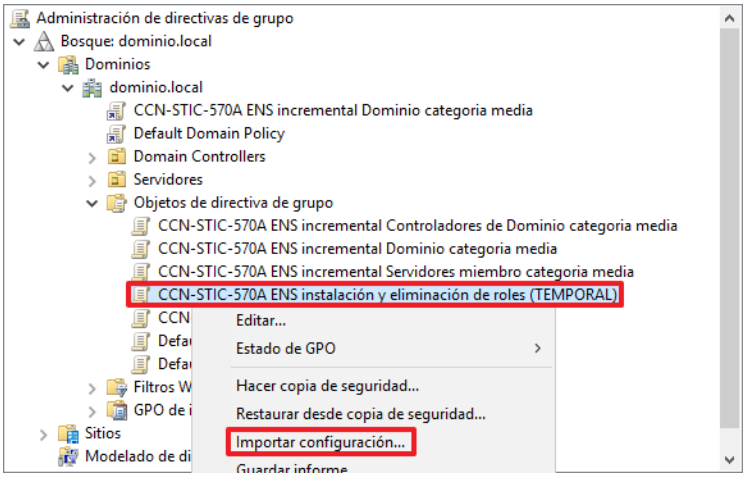
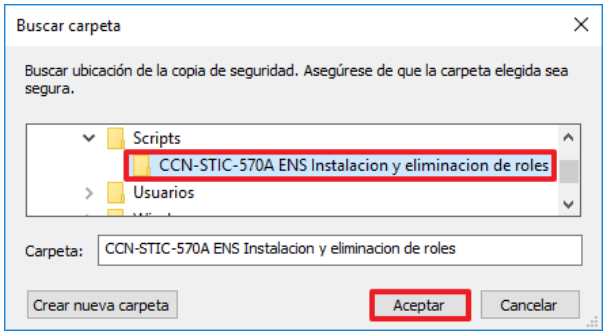
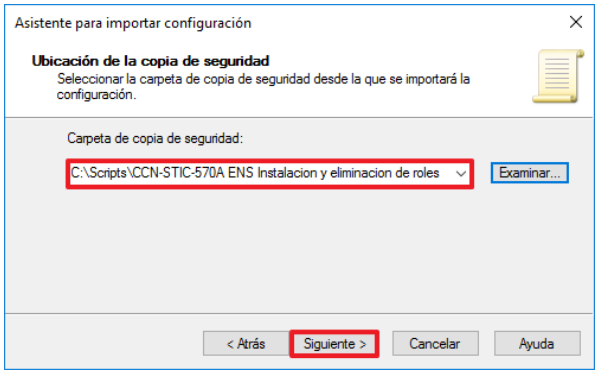
Para instalar o eliminar un rol y/o característica será necesario la creación de una política de seguridad temporal para tal efecto.

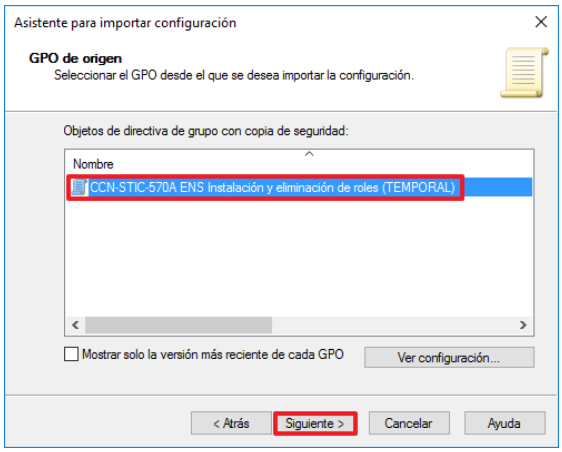
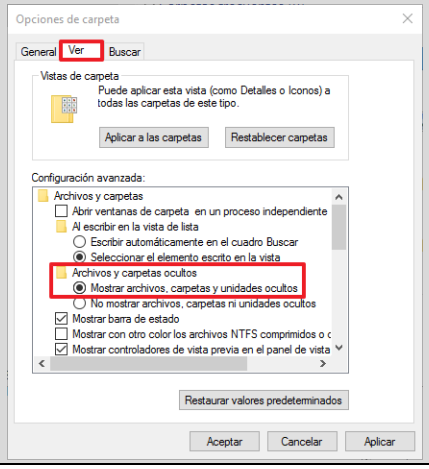
Los pasos que se describen a continuación se realizarán en un controlador de dominio del directorio activo al que va a pertenecer el servidor miembro que se está securizando.

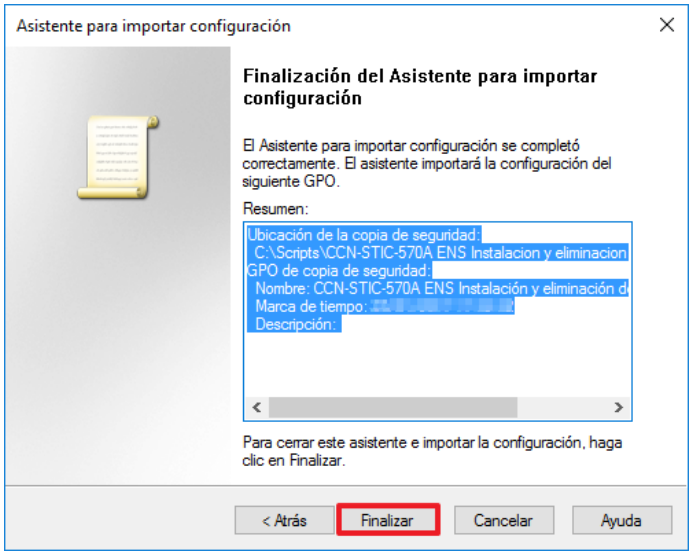
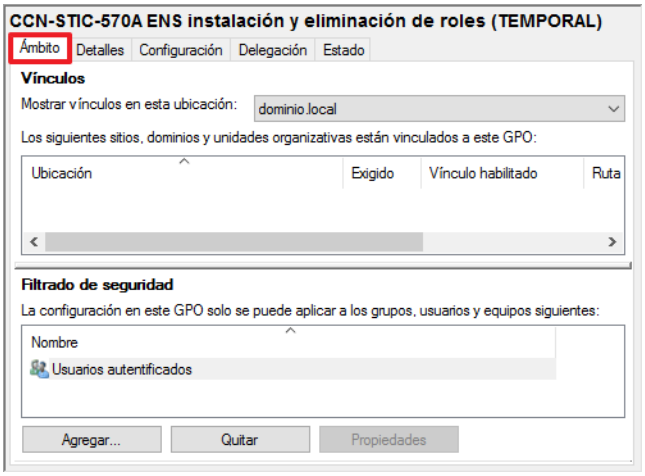
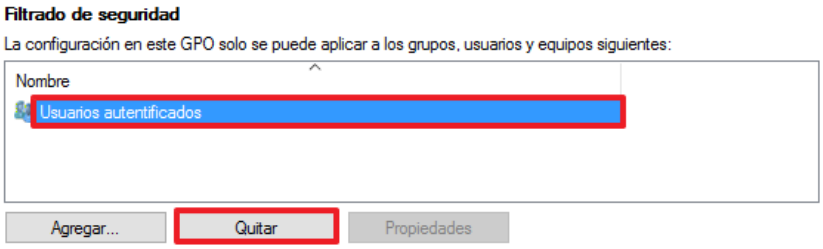
Nota: Recuerde que una vez instalados o eliminados los roles y/o características necesarias deberá aplicar el punto "3.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO".

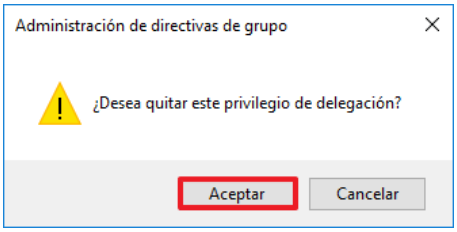
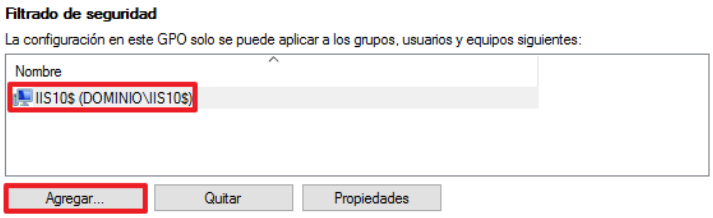
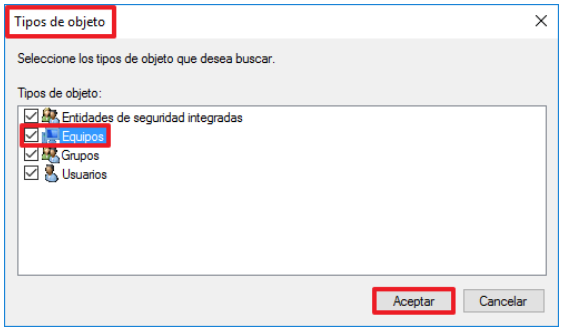
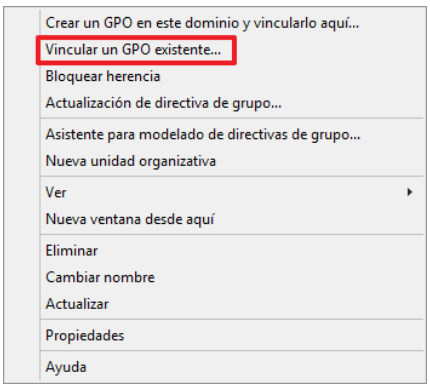
Paso	Descripción
118.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
119.	Cree el directorio "Scripts" en la unidad "C:\". **Nota:** Los scripts asumen que su ubicación en el sistema será bajo "C:\Scripts". Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
120.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".
121.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
122.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Si". 

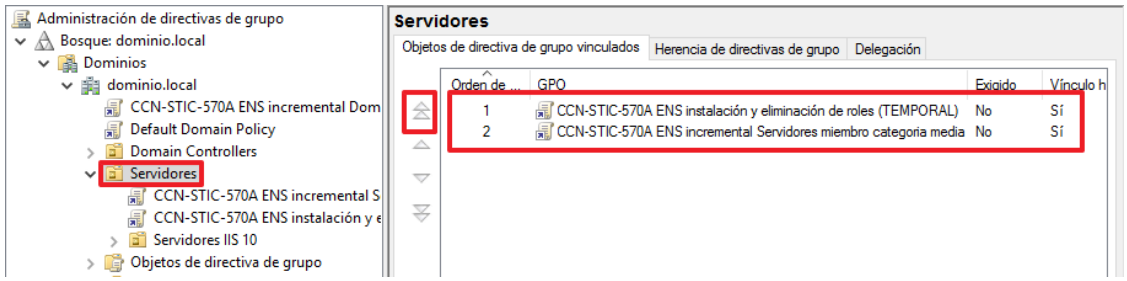
Paso	Descripción
123.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administración de directivas de grupo”** 
124.	Ubíquese sobre el nodo “Objetos de directiva de grupo” ubicado en **“Bosque:<su dominio> → Dominios → <su dominio> → Objetos de directiva de grupo”**.
125.	Si ya estuviese creada la directiva de grupo “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)” deberá continuar a partir del paso 136.
126.	Pulse con el botón derecho, sobre dicha carpeta y seleccione la opción “Nuevo”. 
127.	Introduzca como nombre “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)” y pulse el botón “Aceptar”. 

Paso	Descripción
128.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración…”. 
129.	En el asistente de importación de configuración, pulse el botón “Siguiente >”.
130.	En “Carpeta de copia de seguridad”, pulse el botón “Examinar...”.
131.	Seleccione la carpeta “CCN-STIC-570A ENS Instalación y eliminación de roles” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 
132.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada. 

Paso	Descripción
133.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)” y pulse el botón “Siguiente >”.  **Nota:** Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero “manifest.xml”. Este es un fichero oculto y, por lo tanto, debe mostrar en “opciones de carpeta” la opción “Mostrar archivos, carpetas y unidades ocultos”. 
134.	En la pantalla de examen, pulse el botón “Siguiente >”.

Paso	Descripción
135.	Para completar el asistente pulse el botón “Finalizar”. 
136.	A continuación, seleccione la nueva política de grupo configurada y diríjase a la pestaña “Ámbito” que se encuentra en el panel derecho. 
137.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 

Paso	Descripción
138.	A continuación, pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
139.	Una vez quitado, pulse el botón “Agregar…” y seleccione únicamente los equipos o grupos sobre los que desea aplicar la política de seguridad, para ello es necesario marcar en tipos de objeto, la opción “Equipos”.   **Nota:** En este ejemplo se agrega el equipo IIS10.
140.	A continuación, identifique las unidades organizativas en la que desea instalar o eliminar algún rol y/o característica. Pulse con el botón derecho sobre la unidad organizativa deseada y seleccione la opción del menú contextual “Vincular un GPO existente…”. 

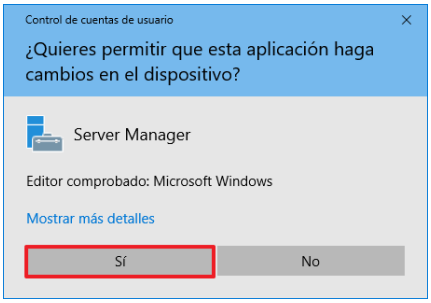
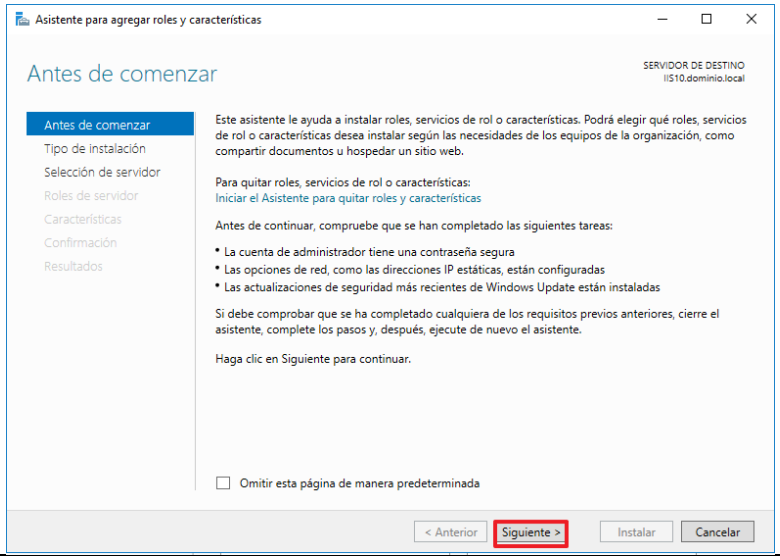
Paso	Descripción
141.	Una vez vinculado, en el panel derecho seleccione la pestaña “Objetos de directiva de grupo vinculados” y seleccione la política “CCN-STIC 570A ENS Instalación y eliminación de roles”
142.	Pulse el botón con la flecha que apunta hacia arriba hasta situar la política “CCN-STIC 570A ENS Instalación y eliminación de roles” en primer lugar dentro del orden de vinculación. 

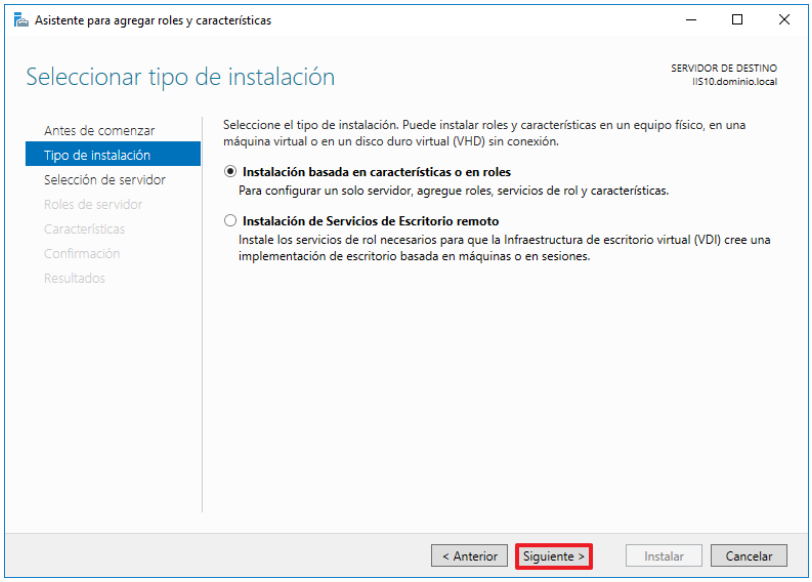
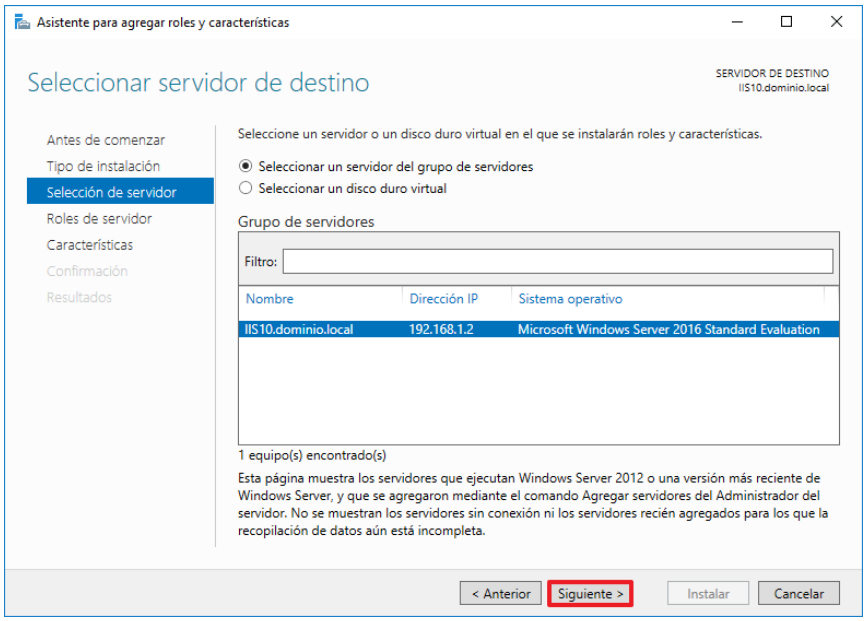
3.2. INSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS

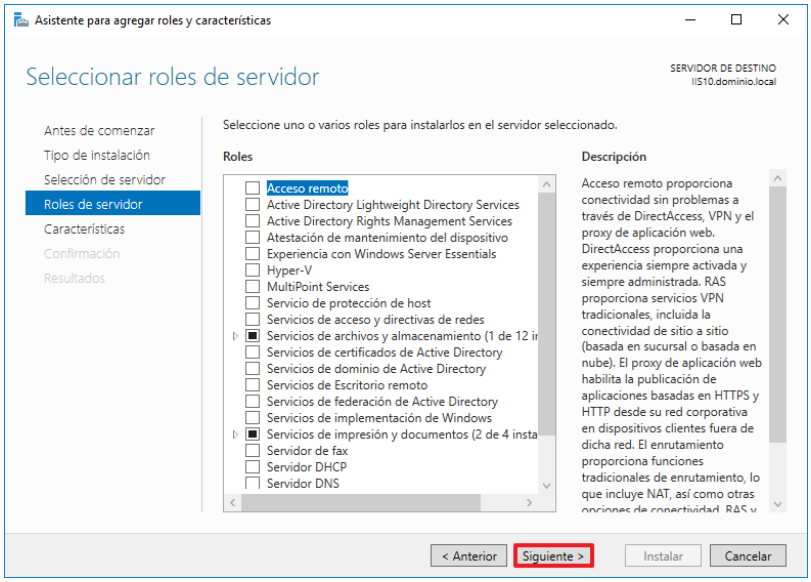
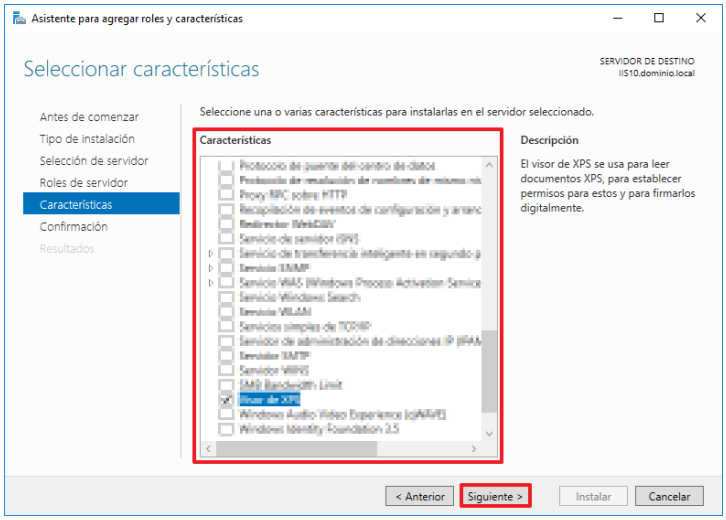
Los pasos que se describen a continuación se realizarán en el servidor miembro del dominio que se está securizando.

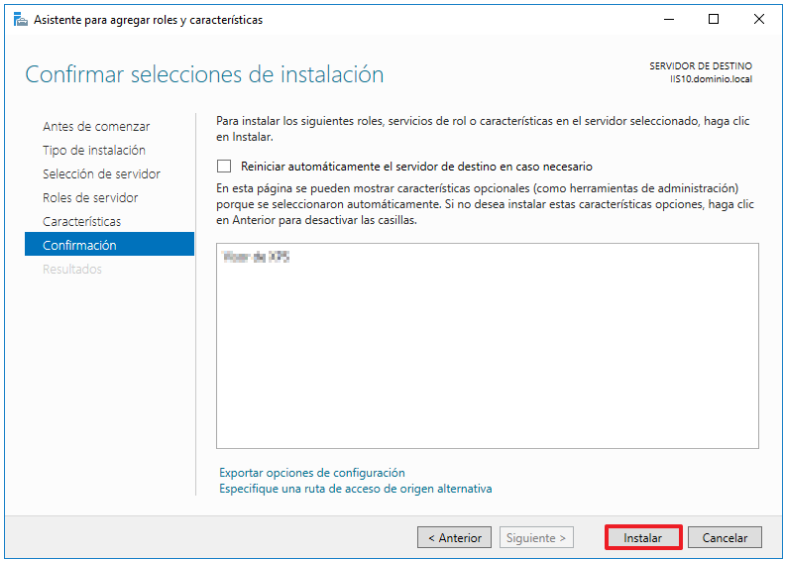
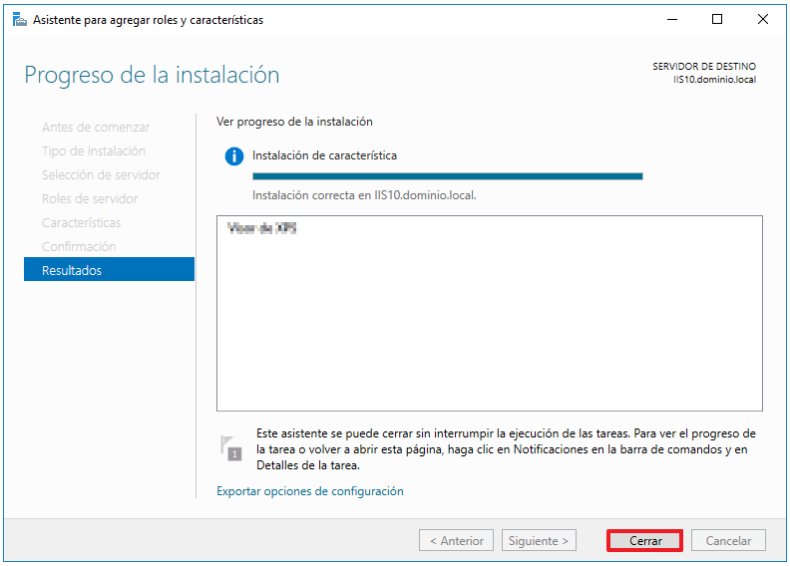
Nota: Para continuar este paso a paso debe haber aplicado previamente el punto “3.1 PREPARACIÓN DEL DIRECTORIO ACTIVO”.

Paso	Descripción
143.	Inicie sesión en el servidor miembro donde vaya a instalar un rol y/o característica.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio o administrador local del equipo.
144.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 

Paso	Descripción
145.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Si”. 
146.	A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Agregar roles y características”. 
147.	Comenzará el asistente para agregar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 

Paso	Descripción
148.	Seleccione el tipo de instalación, “Instalación basada en características o roles” y pulse “Siguiente >” para continuar. 
149.	Seleccione el servidor sobre el cual desea instalar un rol o una característica, y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “IIS10”.

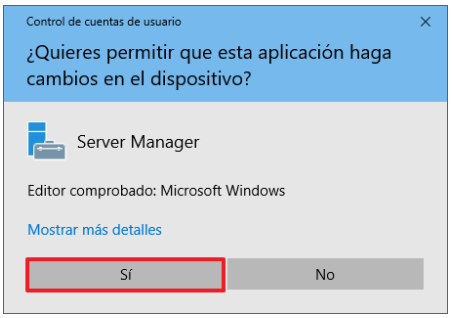
Paso	Descripción
150.	En la siguiente ventana, seleccione los roles que desee instalar en el sistema y pulse “Siguiente >”. 
151.	A continuación, en la siguiente ventana podrá seleccionar las características que desee instalar en el sistema. Seleccione aquellas que desee instalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se instala una característica de prueba. Deberá adaptar este paso a los requerimientos de su organización.

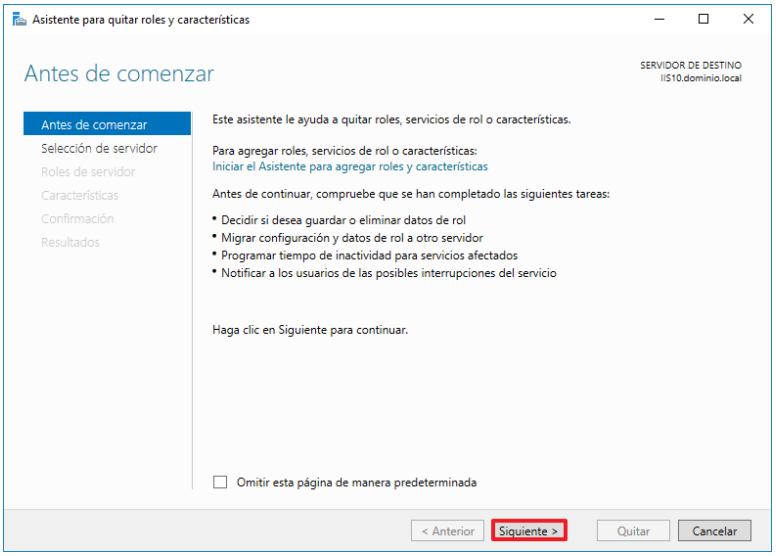
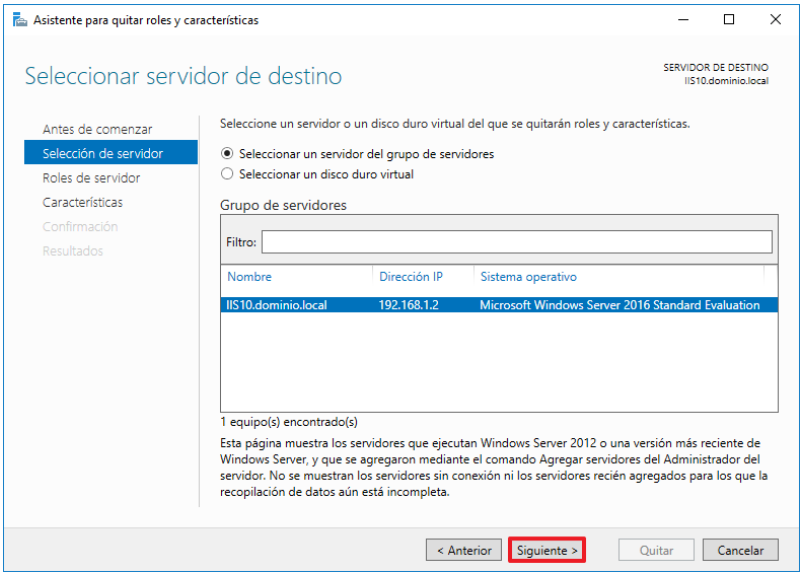
Paso	Descripción
152.	En la ventana “Confirmación” pulse “Instalar” para iniciar el proceso. 
153.	Una vez finalizado el proceso de instalación, pulse sobre “Cerrar” para finalizar la instalación.  **Nota:** En caso de ser necesario, el servidor requerirá un reinicio para finalizar la instalación de roles y características.
154.	Una vez finalizada la instalación de roles y/o características, deberá aplicar el siguiente punto “3.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

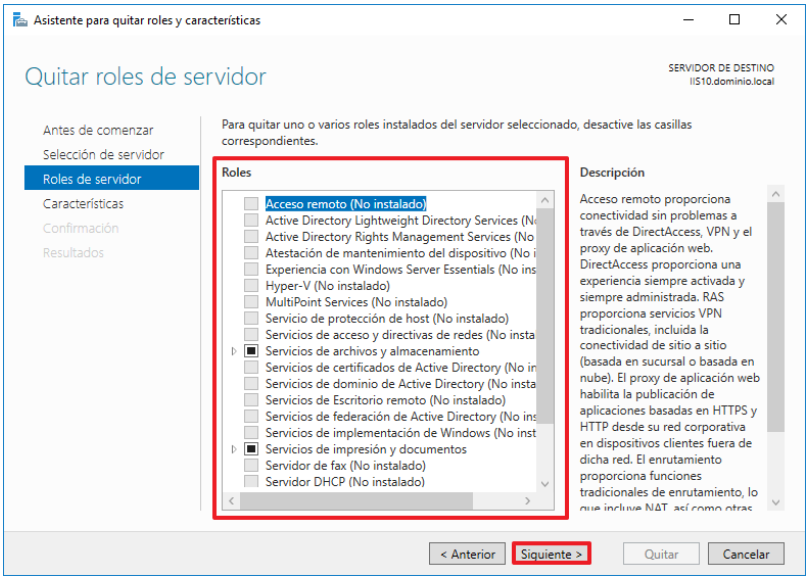
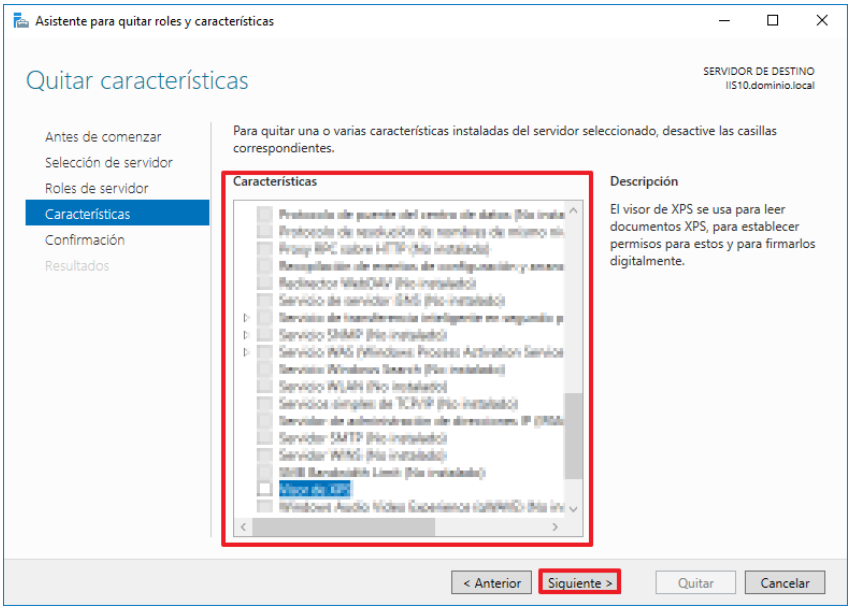
3.3. DESINSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS

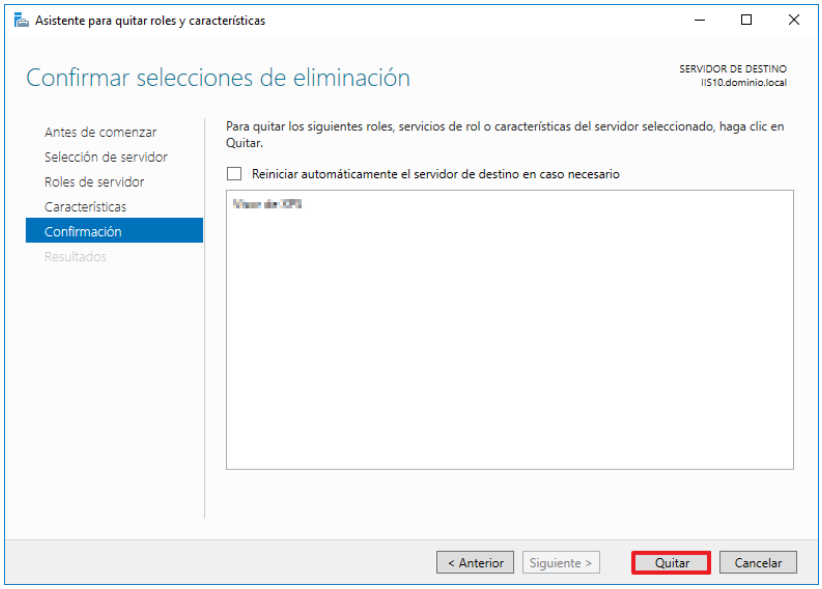
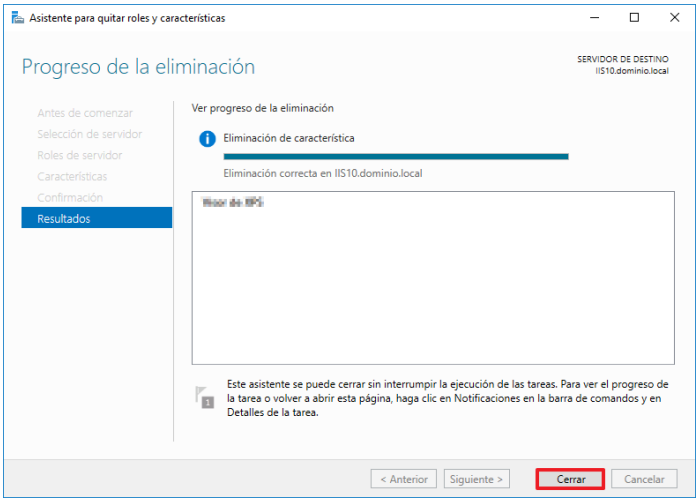
Los pasos que se describen a continuación se realizarán en el servidor miembro del dominio que se está securizando.

Nota: Para continuar este paso a paso debe haber aplicado previamente el punto "3.1 PREPARACIÓN DEL DIRECTORIO ACTIVO".

Paso	Descripción
155.	Inicie sesión en el servidor miembro donde vaya a eliminar un rol y/o característica.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio o administrador local del equipo.
156.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
157.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Si" para continuar. 
158.	A continuación, pulse sobre el botón "Administrar" y seleccione la opción "Quitar roles y funciones". 

Paso	Descripción
159.	Comenzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 
160.	Seleccione el servidor sobre el cual desea eliminar un rol o una característica y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “IIS10”.

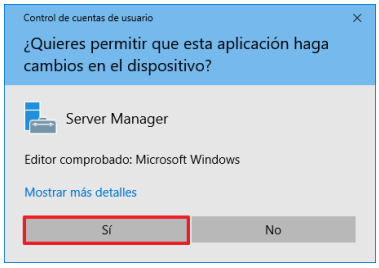
Paso	Descripción
161.	En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Seleccione aquellos que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo no se desinstala ningún rol, deberá adaptar este paso a los requerimientos de su organización.
162.	A continuación, en la siguiente ventana podrá seleccionar las características que desee desinstalar del sistema. Desmarque aquellas que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se desinstala una característica de prueba. Deberá adaptar este paso a los requerimientos de su organización.

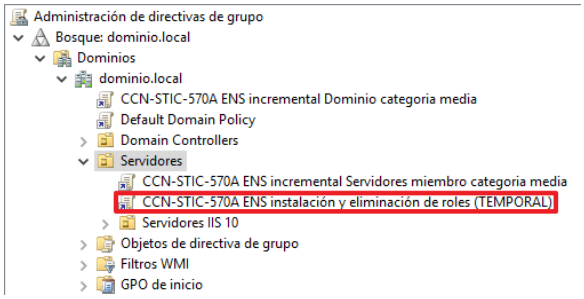
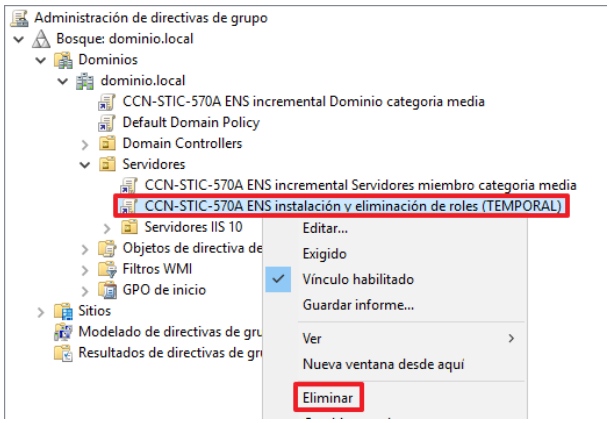
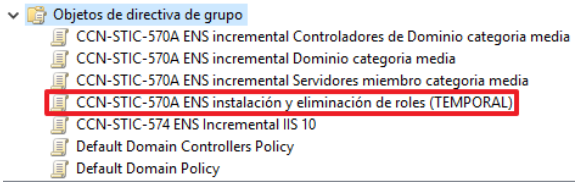
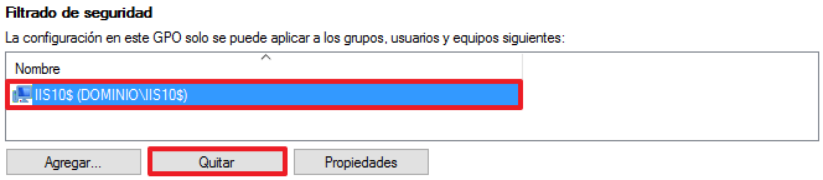
Paso	Descripción
163.	En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso. 
164.	Una vez finalizado el proceso de desinstalación, pulse sobre “Cerrar” para finalizar la desinstalación.  **Nota:** En caso de ser necesario el servidor requerirá un reinicio para finalizar la desinstalación de roles y características.
165.	Una vez finalizada la desinstalación de roles y/o características, deberá aplicar el siguiente paso “3.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

3.4. DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO

Para desvincular o eliminar la GPO “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)” creada en el paso “3.1 PREPARACIÓN DEL DIRECTORIO ACTIVO” deberá implementar el siguiente paso a paso.

Los pasos que se describen a continuación se realizarán en un controlador de dominio del domino al que va a pertenecer el servidor miembro que se está securizando.

Paso	Descripción
166.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
167.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
168.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Si”. 
169.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administración de directivas de grupo”** 

Paso	Descripción
170.	Localice la unidad organizativa donde se está aplicando la GPO “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)”. 
171.	Pulse botón derecho sobre la GPO y seleccione la opción del menú contextual “Eliminar”. 
172.	A continuación, seleccione la política de grupo “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)” ubicada en el contenedor “Objetos de directiva de grupo” y diríjase a la pestaña “Ámbito” que se encuentra en el panel derecho. 
173.	En la opción “Filtrado de seguridad”, Seleccione los equipos o grupos sobre los que se está aplicando la política de seguridad y pulse sobre el botón “Quitar”.  **Nota:** En este ejemplo se elimina el equipo “IIS10”

ANEXO A.3.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA MEDIA DEL ENS PARA SERVIDORES IIS 10 SOBRE MICROSOFT WINDOWS SERVER 2016 EN ENTORNO DE DOMINIO

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores IIS 10 sobre Microsoft Windows Server 2016 con implementación de seguridad de categoría media del ENS.

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

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar la sección de la guía "ANEXO A.3.1 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 MIEMBROS DEL DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS"

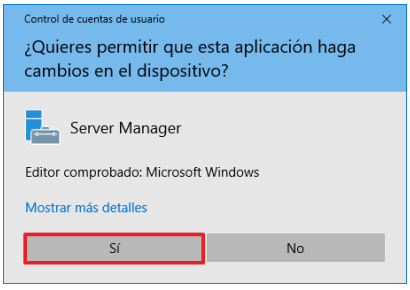
1. COMPROBACIONES EN CONTROLADOR DE DOMINIO

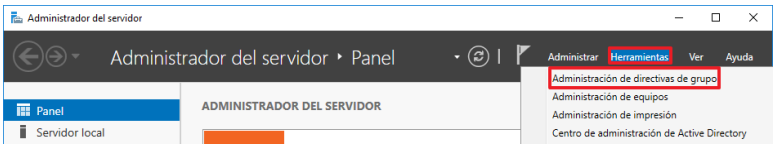
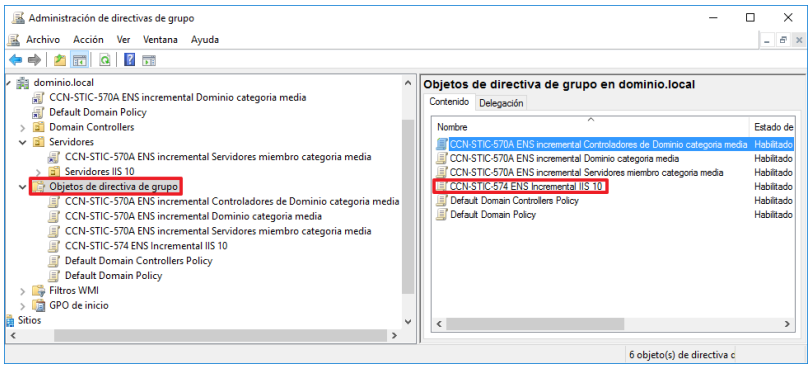
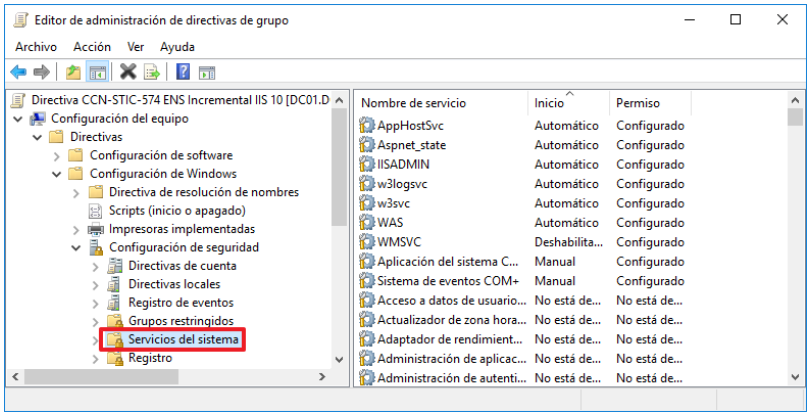
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador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

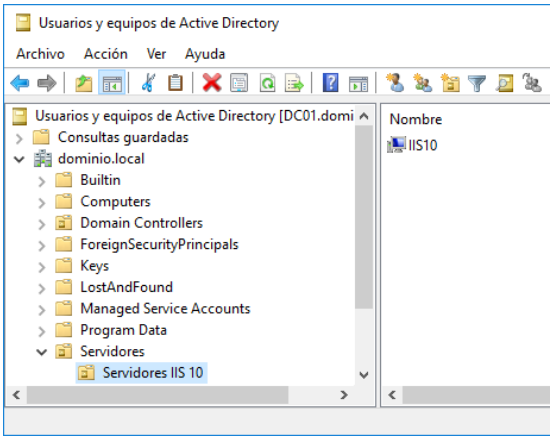
a) Usuarios y equipos de Active Directory (dsa.msc).

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

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

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio.		Inicie sesión con una cuenta que tenga privilegios de administración del dominio. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Pulse "Sí" en la ventana de "Control de cuentas de usuario". 

Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que los objetos de directivas de grupo han sido creados y están habilitados.		Ejecute la herramienta "Administrador de directivas de grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"**  Dentro de la consola diríjase a los "Objetos de directiva de grupo": "**Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo**" Verifique que están creados los tres objetos de directiva de grupo "CCN-STIC-574 ENS Incremental IIS 10", y que en la columna "Estado de GPO" figuran como habilitadas. 
3. Verifique los valores de los servicios del sistema de la directiva CCN-STIC-574 ENS Incremental IIS 10		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-574 ENS Incremental IIS 10" tiene los siguientes valores de servicios de sistema dentro de: **"Directiva CCN-STIC-574 ENS Incremental IIS 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"**. 

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**Permiso**	**OK/NOK**
Servicio auxiliar de host para aplicaciones		AppHostSvc	Automático		
ASP.NET State Service		Aspnet_state	Automático		
Aplicación del sistema COM+		COMSysApp	Manual		
Servicio de administración IIS		IISADMIN	Automático		
Servicio de registro de W3C		w3logsvc	Automático		
Servicio de publicación World Wide Web		w3svc	Automático		
Servicio WAS		WAS	Automático		
Servicio de Administración Web		WMSVC	Manual		
4. Verifique que los servidores de IIS 10 están dentro de las Unidades Organizativas correspondientes		Utilice la herramienta Usuarios y equipos de Active Directory (“**Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**”) y seleccione las unidades organizativas que contienen los Servidores IIS 10. **Nota:** Para el desarrollo de esta guía se utiliza la Unidad Organizativa “Servidores IIS 10”. 			

2. COMPROBACIONES EN SERVIDOR MIEMBRO

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

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

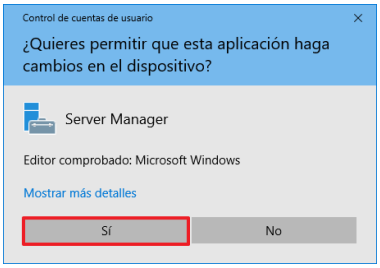
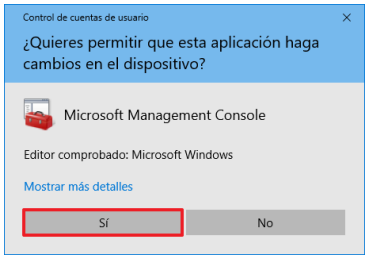
a) Administrador del Servidor

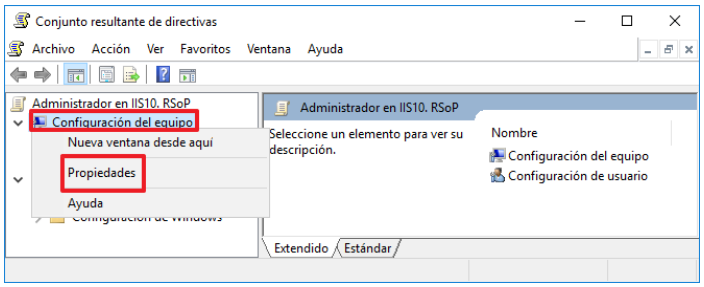
b) Conjunto resultante de directivas (rsop.msc)

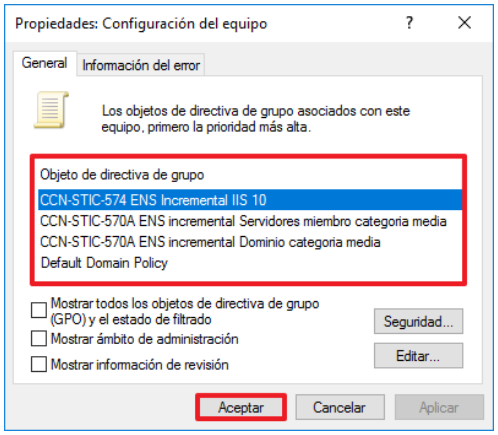
c) Consola de servicios (services.msc)

d) Editor de registro (regedit.exe)

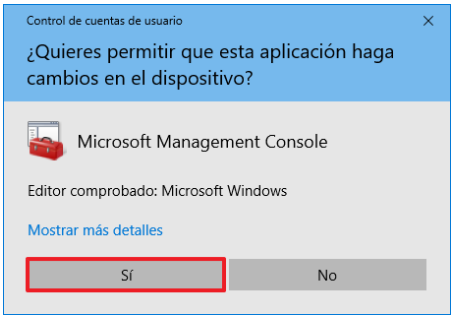
e) Explorador de Archivos (explorer.exe)

Comprobación	OK/NOK	Cómo hacerlo
5. Inicie sesión en el servidor a comprobar.		En uno de los servidores miembro del dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Pulse "Sí" en la ventana de "Control de cuentas de usuario". 
6. Verifique que el equipo ha recibido la directiva de grupo CCN-STIC-574 ENS incremental IIS 10.		Ejecute la consola de administración "Conjunto resultante de directivas", para ello, pulse **"Tecla Windows+R → rsop.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" en la ventana que se muestra a continuación. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>
Seleccione en ella la rama "Configuración del equipo", márquela con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la figura.


En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", resaltada en la siguiente figura.


Verifique que en dicha sección aparecen listados, y por ese orden, los objetos de directiva de grupo que se indican en la siguiente tabla:
<table>
<tr><th>Objeto de directiva de grupo</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-574 ENS incremental IIS 10</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS incremental Servidores miembro categoria media</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS incremental Dominio categoria media</td><td></td></tr>
<tr><td>Default Domain Policy</td><td></td></tr>
</table>
</td></tr>
</table>

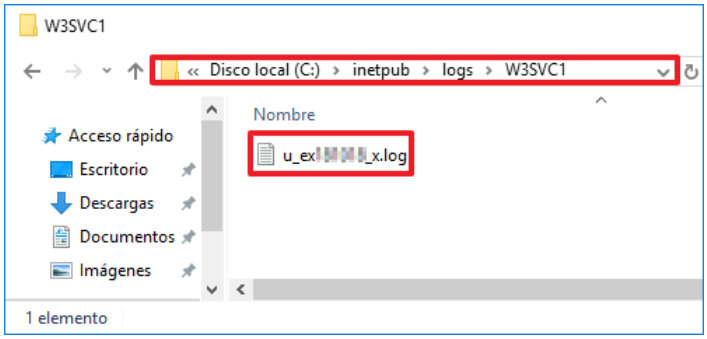
Comprobación	OK/NOK	Cómo hacerlo
7. Verifique que los servicios del sistema están correctamente configurados		Usando la consola de servicios (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → services.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" para continuar.  Verifique que el tipo de inicio de los servicios que aparecen en el sistema y en la siguiente tabla coinciden: **Nota:** Dependiendo de las características de IIS 10 instaladas en el equipo es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio auxiliar de host para aplicaciones	AppHostSvc	Automático		
ASP.NET State Service	Aspnet_state	Automático		
Aplicación del sistema COM+	COMSysApp	Manual		
Servicio de administración IIS	IISADMIN	Automático		
Servicio de registro de W3C	w3logsvc	Automático		
Servicio de publicación World Wide Web	w3svc	Automático		
Servicio WAS	WAS	Automático		
Servicio de Administración Web	WMSVC	Manual		

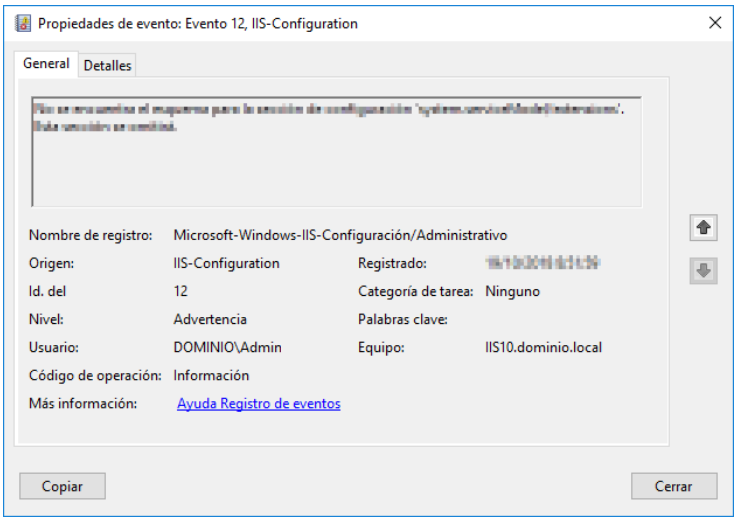
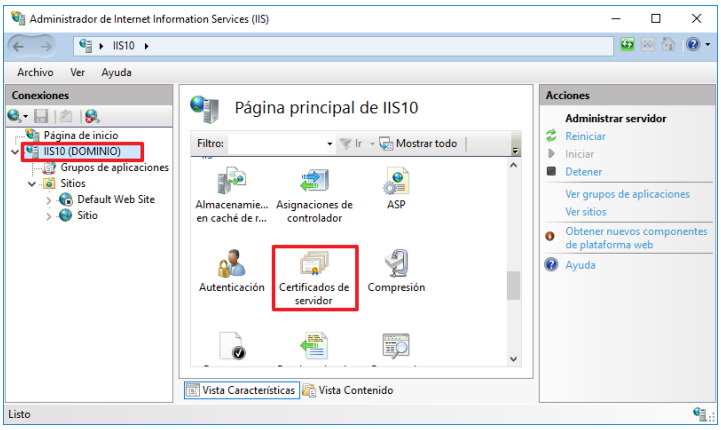
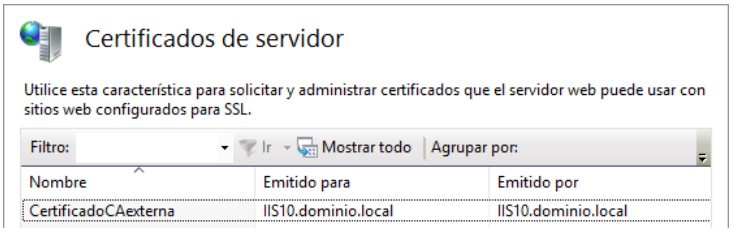
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>8. Verifique que se han asignado los permisos correctos en el sistema de archivos</td><td></td><td>Utilizando el Explorador de Windows:
“Windows+R → Explorer”
En caso de no saber dónde apunta cada una de las rutas abreviadas que se especifica, ejecute Explorer <<ruta>> donde <<ruta>> se sustituirá por la ruta abreviada.

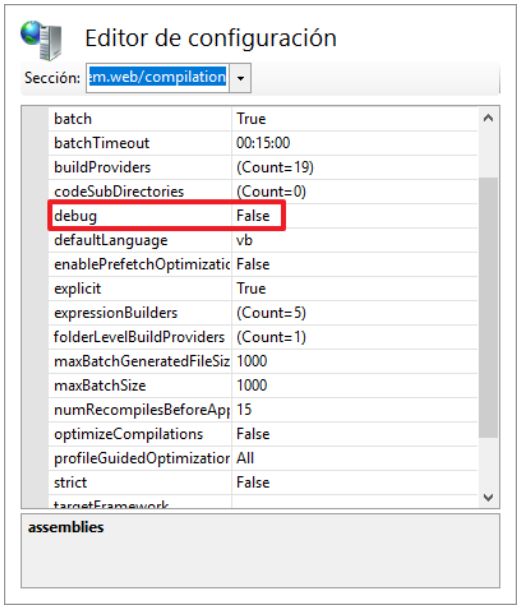
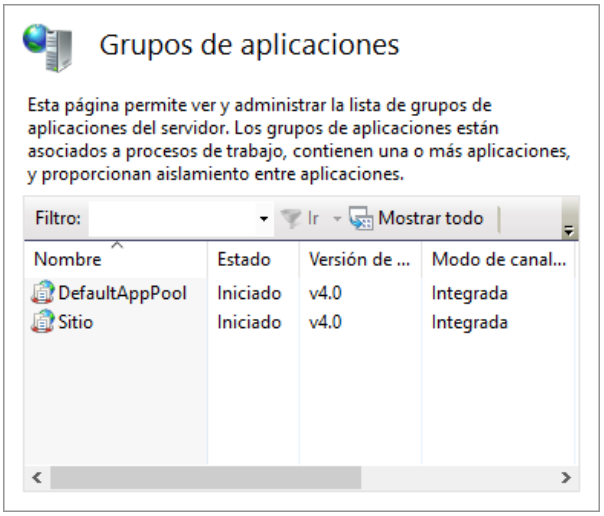
Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, marcándolo con el botón derecho y eligiendo la opción “Propiedades” del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá situarse en la pestaña “Seguridad”. En la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios.
Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados.</td></tr>
</table>

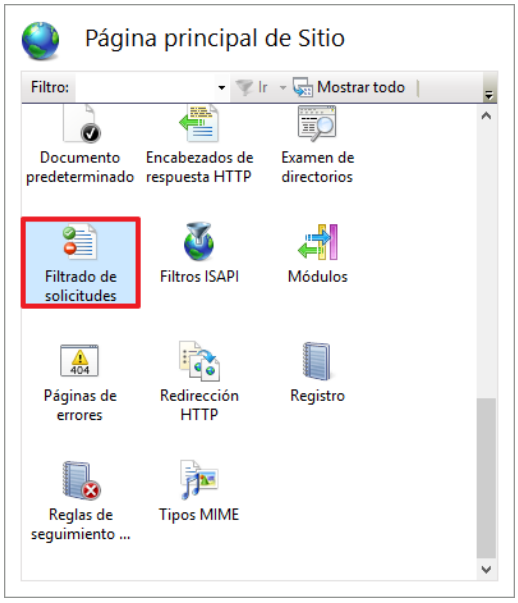
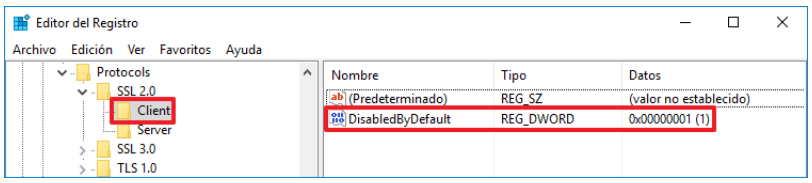
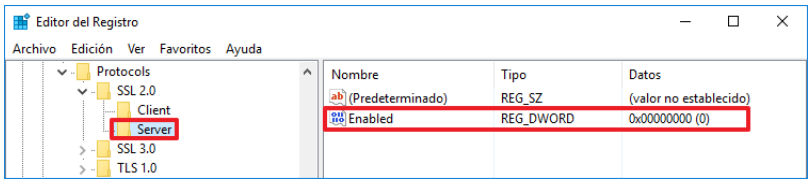
Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\inetsrv\MetaBack	Administrador	Control total	
	System	Control total	
%SystemRoot%\LogFiles	Administrador	Control total	
	System	Control total	
	Creator Owner	Control total	

<table>
<tr><td>9. Compruebe que el registro de acceso de IIS está operativo.</td><td></td><td>En la configuración que ha realizado ha habilitado el registro de acceso al servidor, por lo que debe asegurarse que está registrando la actividad. Para ello verifique que el directorio C:\inetpub\logs\W3SVC1\ contiene ficheros con el formato u_exfecha.log. Abriendo el último deberá ver que registra los accesos correctamente.
 

Nota: Tenga en cuenta que no se crea ningún registro hasta que no se realiza alguna actividad.</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
10. Verifique que los registros son actuales		Los dos registros deben contener eventos, abra ambos y compruebe que las últimas fechas de registro son recientes. 
11. Comprobación certificado sitio web HTTPS		Dentro de la consola del "Administrador de Internet Information Services (IIS)" accedemos a "Certificados de servidor".   **Nota:** No olvide estar posicionado sobre el nombre del servidor y no sobre un determinado sitio o carpeta virtual, ya que todas las comprobaciones que está haciendo desde la consola de administración de IIS están siendo sobre el servidor. Se recomienda el uso de certificados EV en la categoría media del ENS

Comprobación	OK/NOK	Cómo hacerlo
12. Comprobación de la depuración de sistemas en producción		Compruebe que la depuración en sistemas de producción esta deshabilitada. Para ello chequee: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS) → [nombre_del_servidor] → Sitios → Editor de configuración → Sección: System.web → Compilation → Debug → False"**. 
13. Comprobación de las identidades del grupo de aplicaciones		Compruebe que en las identidades del grupo de aplicaciones no hay identidades de servicio integradas. Para ello chequee: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS) → [nombre_del_servidor] → Grupo de aplicaciones"**. 

Comprobación	OK/NOK	Cómo hacerlo
14. Comprobación del filtrado de solicitudes		Compruebe que está habilitado el filtrado de solicitudes. Para ello chequee: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS) → [nombre_del_servidor] → Filtrado de solicitudes"**. 
15. Compruebe que se encuentran deshabilitados los algoritmos SSL2, SSL3 y TLS 1.0.		Compruebe que el uso de los algoritmos SSL2, SSL3 y TLS 1.0 estén deshabilitados. Utilizando el Explorador de Windows: **"Windows+R → Regedit.exe"** Y a continuación diríjase a: "**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols"** Compruebe que existen las carpetas con los 3 algoritmos y que contienen las carpetas Client y Server. Compruebe el contenido de la carpeta Client tal y como se muestra a continuación.  Compruebe el contenido de la carpeta Server tal y como se muestra a continuación. 

ANEXO A.3.3. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 INDEPENDIENTES SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tenga que securizar IIS 10 sobre Microsoft Windows Server 2016 independientes con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría media, deberá realizar las implementaciones según se referencian en el presente anexo.

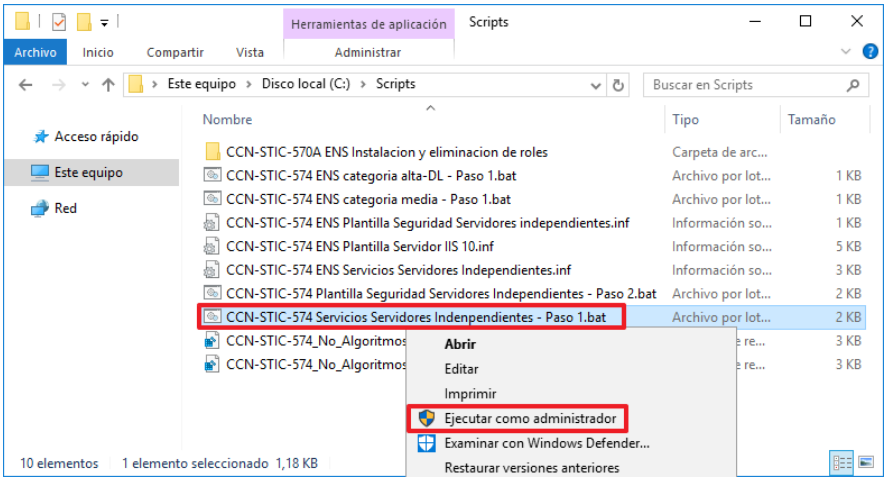
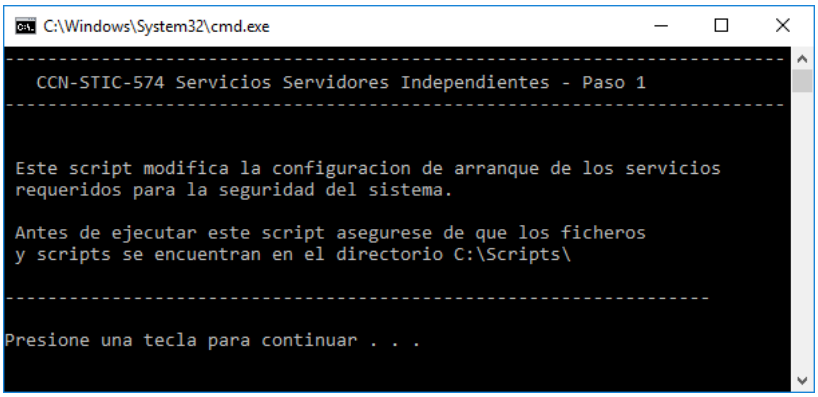
Debe tener en consideración que, antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

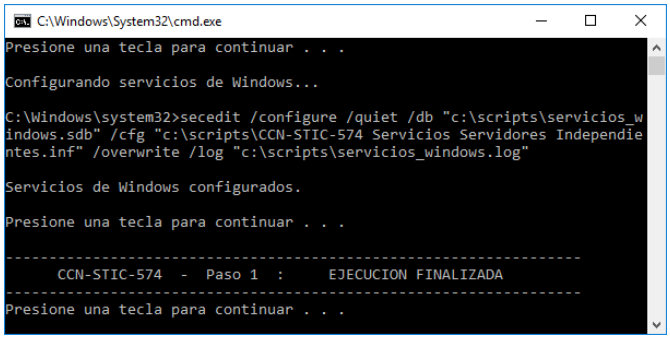
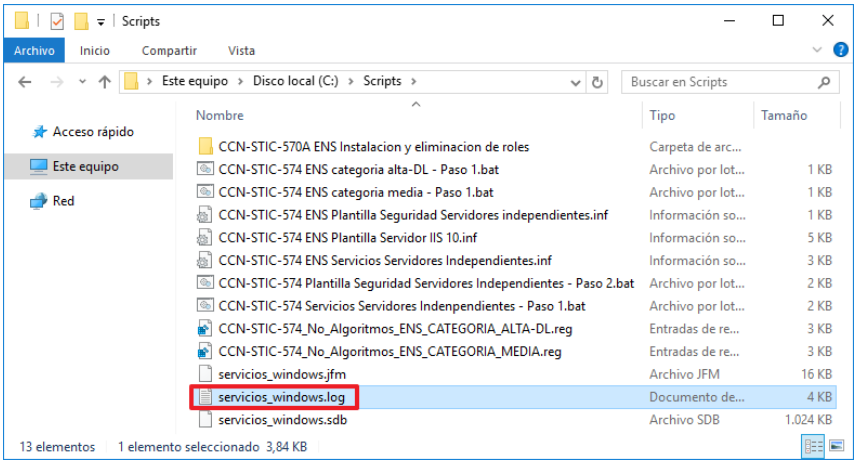
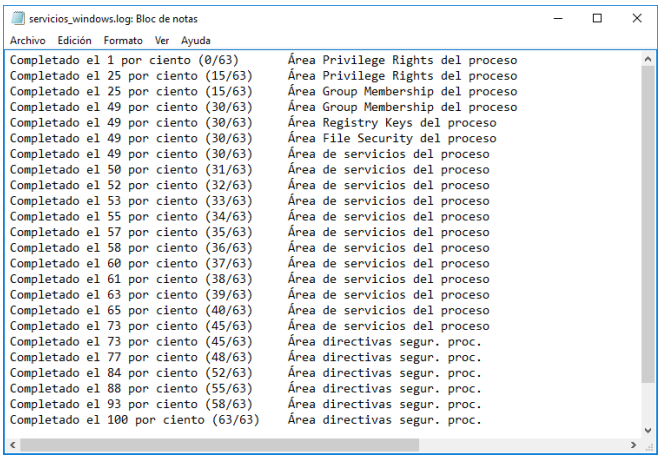
Nota: Si instala Internet Information Services por primera vez con la guía 570A o 570B aplicada debe habilitar la instalación remota de roles, características y servicios de rol a través de Shell la cual se encuentra deshabilitada por LGPO.
Si ha instalado el rol de IIS después de haber aplicado el procedimiento descrito en las guías mencionadas anteriormente, deberá volver a aplicar dicho paso a paso antes de continuar con la presente guía. Esto es debido a que durante la instalación del rol se modifican los permisos de usuario del sistema y altera el nivel mínimo de seguridad establecido por el ENS.

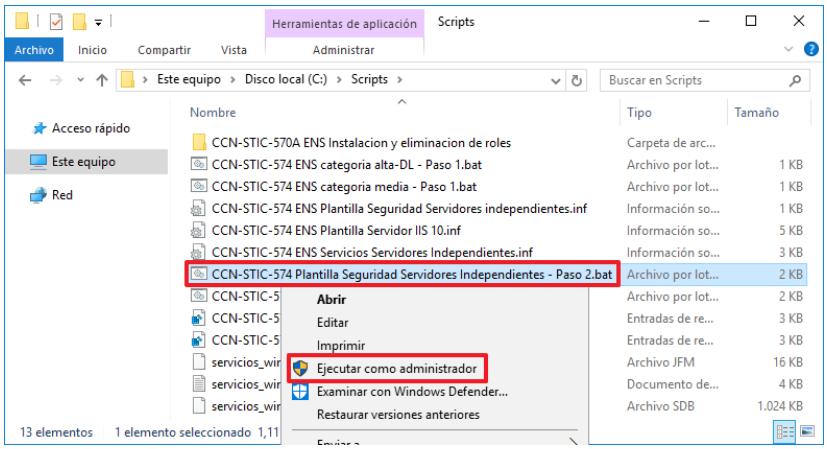
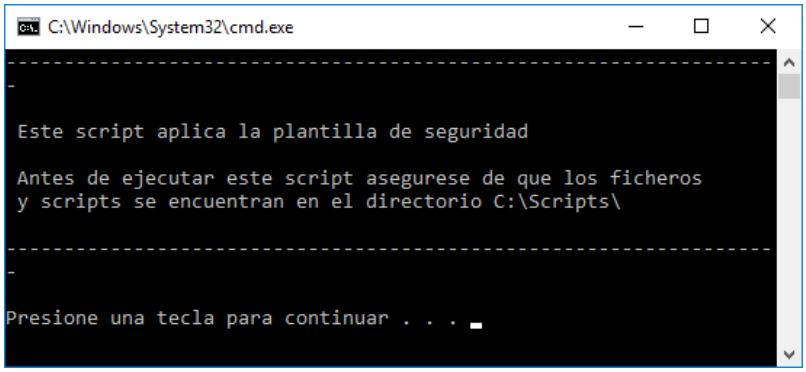
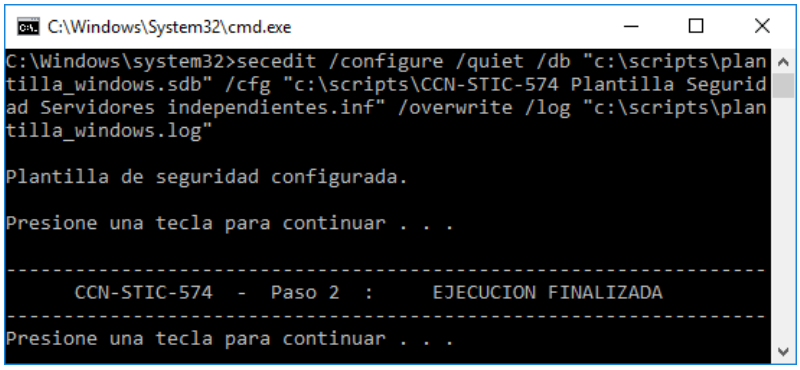
1. CONFIGURACIÓN DE LA SEGURIDAD LOCAL

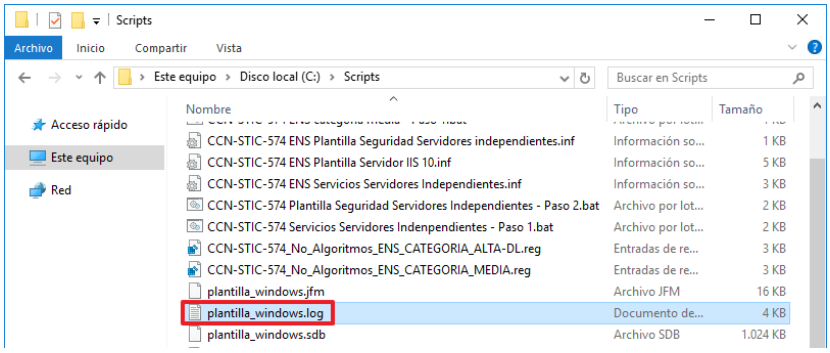
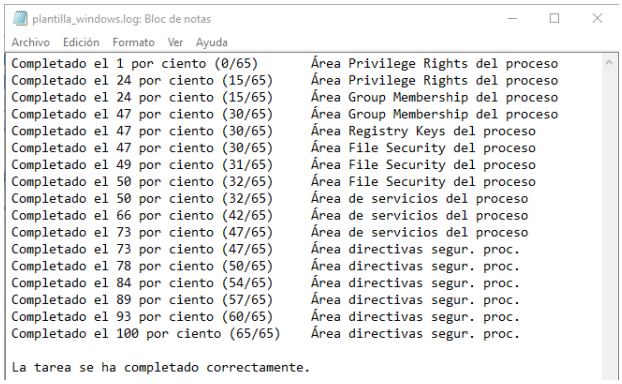
Los pasos que se describen a continuación se realizarán en todos aquellos servidores IIS 10 sobre Microsoft Windows Server 2016, independientes, que implementen servicios o información de categoría media y que se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

Paso	Descripción
1.	Inicie sesión en el servidor independiente donde se va aplicar seguridad según criterios de ENS. 
2.	Debe iniciar sesión con una cuenta que sea administrador del servidor.

Paso	Descripción
3.	Cree el directorio “Scripts” en la unidad “C:\”.
4.	Copie los scripts asociados a esta guía en el directorio “C:\Scripts”.
5.	Abra la carpeta C:\Scripts y pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-574 Servicios Servidores Independientes – Paso 1.bat” y seleccione la opción “Ejecutar como administrador”.  **Nota:** En función del usuario con el que se haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que se le solicite la elevación de privilegios. Para ello introduzca las credenciales de un usuario con permisos de administrador o bien eleve automáticamente los privilegios sin necesidad de introducir usuario y contraseña.
6.	Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la categoría media del ENS. 

Paso	Descripción
7.	Una vez completado el proceso, deberá pulsar una tecla para continuar. 
8.	Pulse de nuevo otra tecla, para finalizar la ejecución del script. La ejecución del script genera un registro en la carpeta “C:\Scripts” con el nombre de “servicios_windows.log”. 
9.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación. 

Paso	Descripción
10.	A continuación, pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-574 Plantilla Seguridad Servidores Independientes - Paso 2.bat” y seleccione la opción “Ejecutar como administrador”.  **Nota:** En función del usuario con el que se haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que se le solicite la elevación de privilegios. Para ello introduzca las credenciales de un usuario con permisos de administrador o bien eleve automáticamente los privilegios sin necesidad de introducir usuario y contraseña.
11.	Pulse una tecla para iniciar la ejecución del script que configurará la plantilla de seguridad con la seguridad requerida para la categoría media del ENS. 
12.	Una vez completado el proceso, deberá pulsar una tecla para continuar. 

Paso	Descripción
13.	Pulse de nuevo otra tecla, para finalizar la ejecución del script, este genera un registro en “C:\Scripts” con el nombre de “plantilla_windows.log”. 
14.	Abra este registro para comprobar si la configuración de la plantilla ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación. 

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración. Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría media.

No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

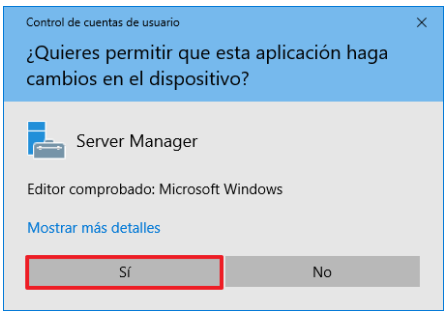
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

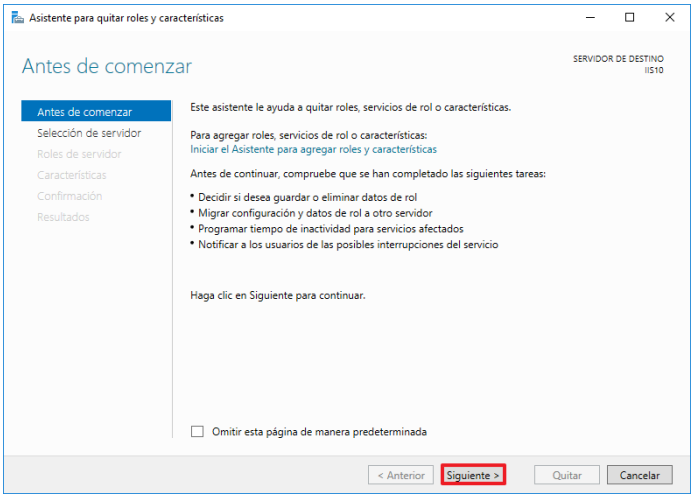
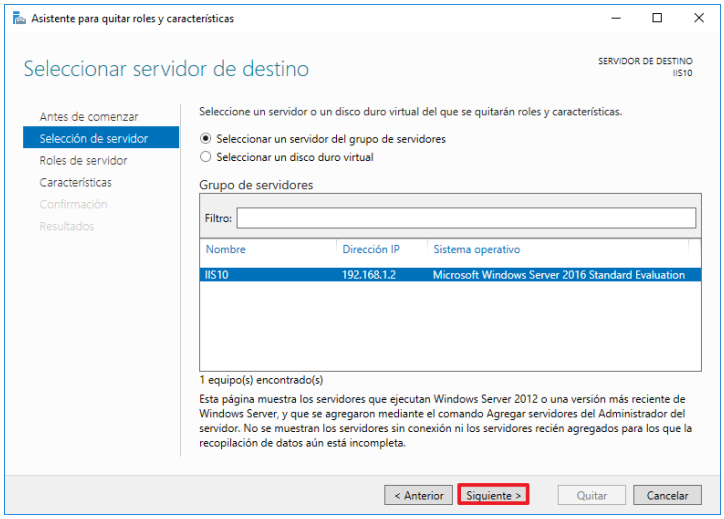
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

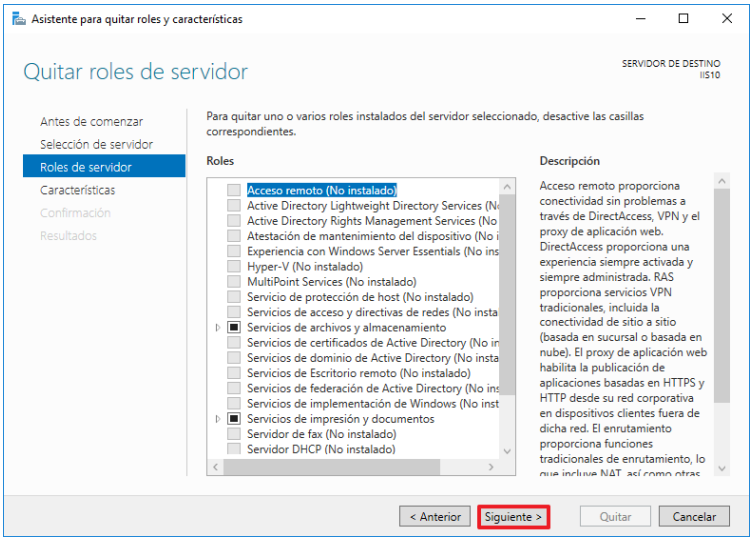
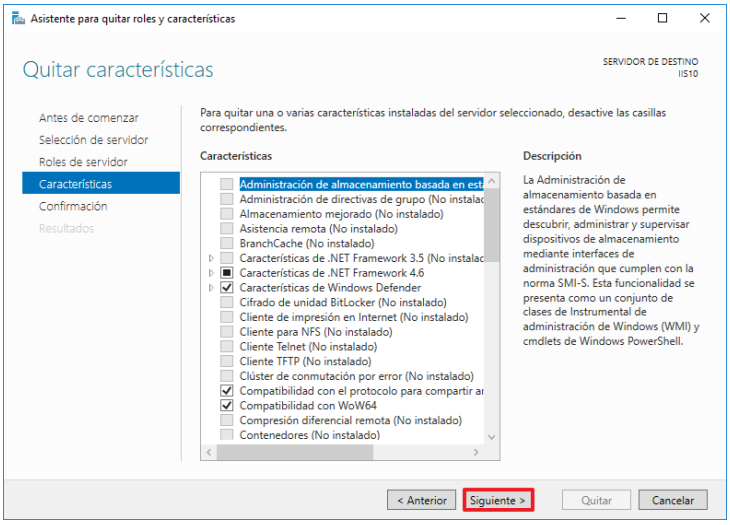
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

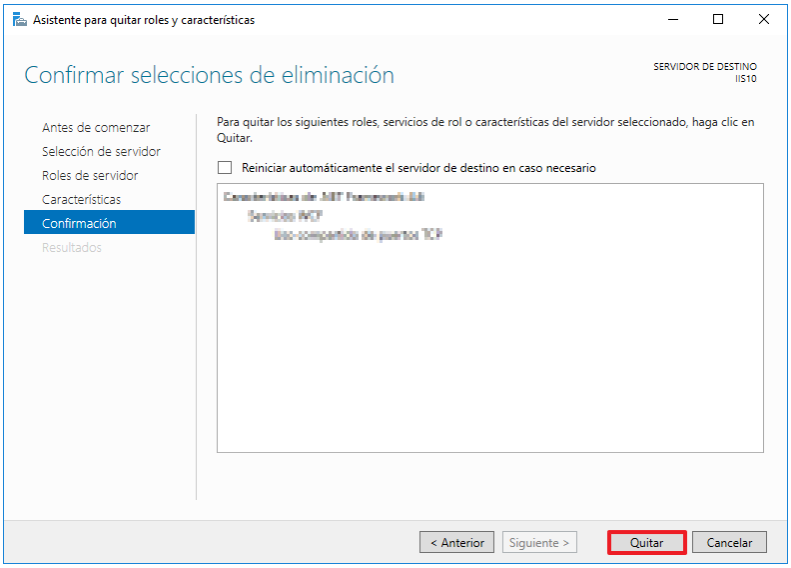
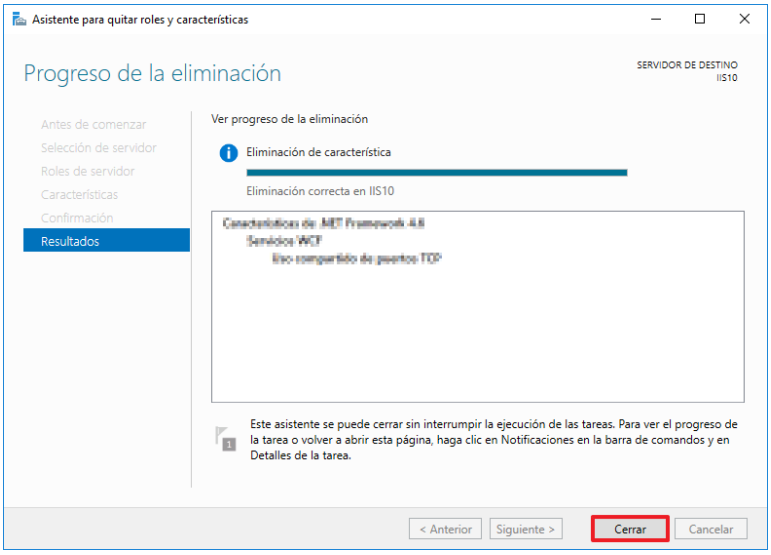
Es recomendable que el sitio web este alojado en otra ubicación de disco diferente a la del sistema operativo y que esta solo se utilice para el alojamiento de sitios web, evitando con ello exponer más información de la estrictamente necesaria.

Para realizar el siguiente paso a paso deberá realizar previamente el paso “3.1 PREPARACIÓN DEL SERVIDOR INDEPENDIENTE” y una vez finalizado deberá realizar el paso “3.4 DESHABILITACIÓN DE UNA DIRECTIVA DE GRUPO LOCAL”.

Paso	Descripción
15.	A continuación, deberá iniciar sesión en el servidor independiente donde está instalado el rol de IIS 10. 
16.	Pulse sobre el administrador del servidor. 
17.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar. 

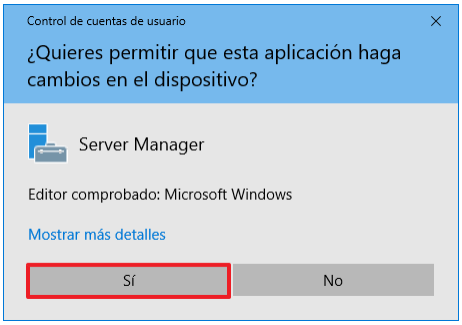
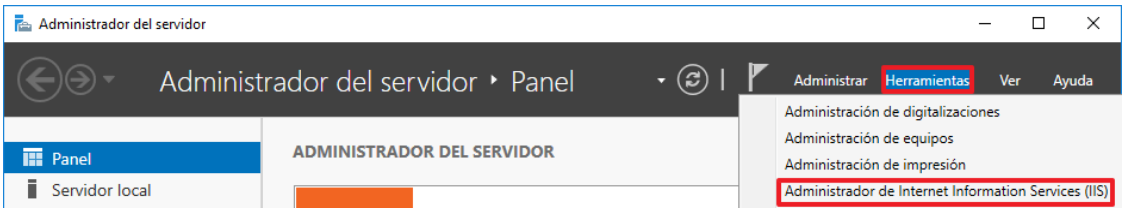
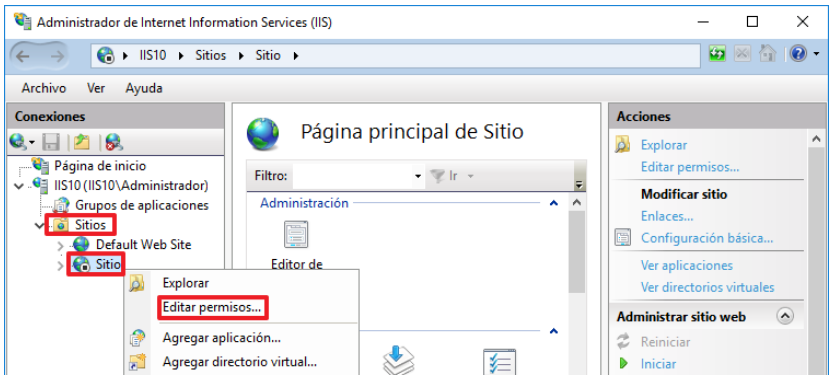
Paso	Descripción
18.	A continuación, pulse sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione **"Administrar → Quitar roles y funciones"** 
19.	Comenzará el asistente para quitar roles y características, pulse sobre el botón "Siguiente >". 
20.	Seleccione el servidor donde desea quitar las características del IIS 10 y pulse siguiente. 

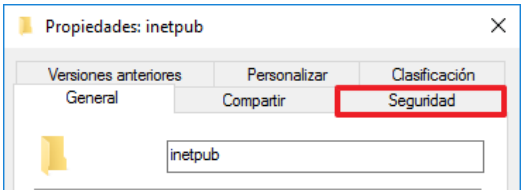
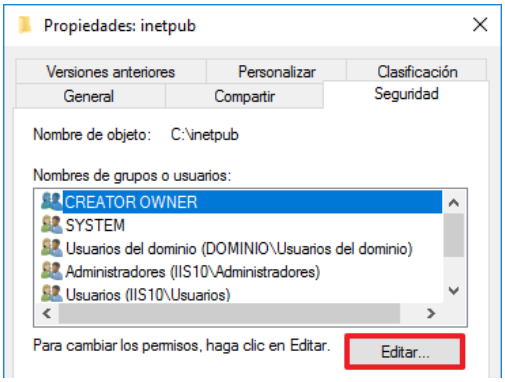
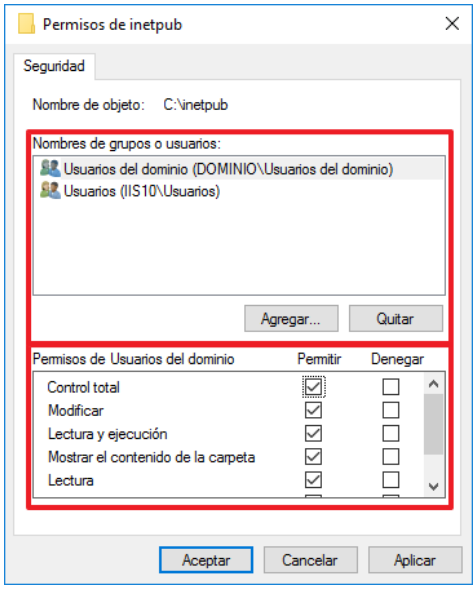
Paso	Descripción
21.	En la siguiente ventana podrá quitar roles del servidor, en este caso pulse siguiente para acceder a las características de los roles instalados. 
22.	A continuación, seleccione las características que desea quitar. 

Paso	Descripción
23.	La siguiente pantalla mostrara las características a modos resumen que desea quitar, confirme que las características seleccionadas son las correctas y pulse “Quitar”. 
24.	Una vez finalizada la desinstalación pulse “Cerrar”.  **Nota:** Debe tener en cuenta que la desinstalación de determinadas características puede requerir el reinicio del equipo.

2.2. GESTIÓN DE PERMISOS RECURSOS WEB

En este apartado se tendrá en consideración la gestión y administración del acceso a los recursos web según el marco operacional de categoría media establecido por el ENS, para con ello limitar y controlar el acceso a directorios con información sensible de ser sustraída.

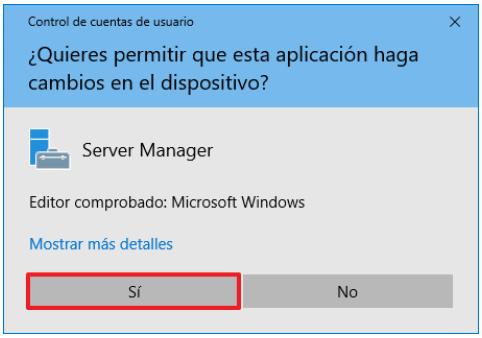
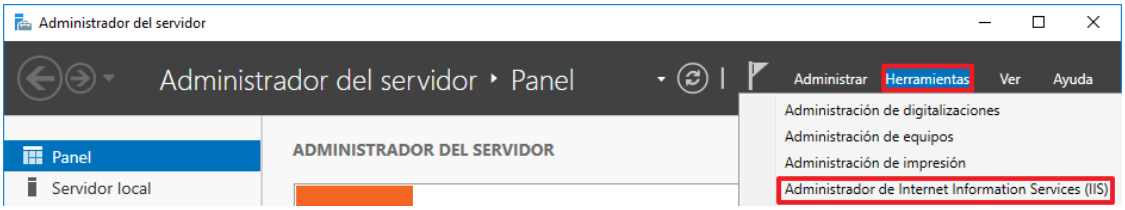
Paso	Descripción
25.	Inicie sesión en el servidor independiente donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
26.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 
27.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione: **“Herramientas → Administrador de Internet Information Services (IIS)”** 
28.	Pulse botón derecho sobre el sitio al cual quiere asignar o quitar permisos. 

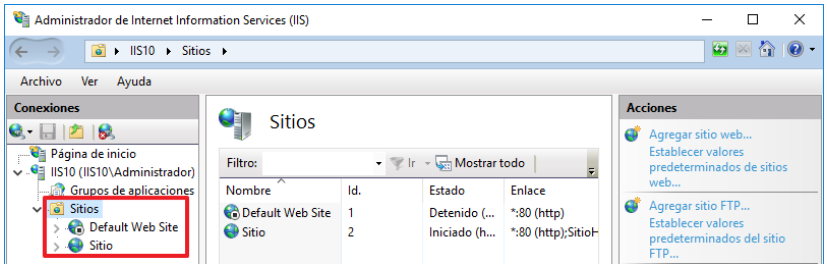
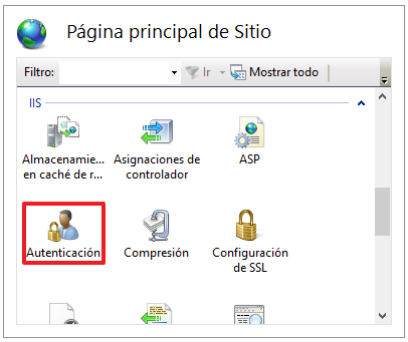
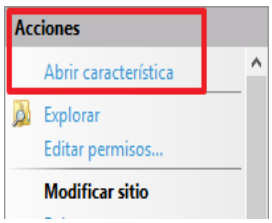
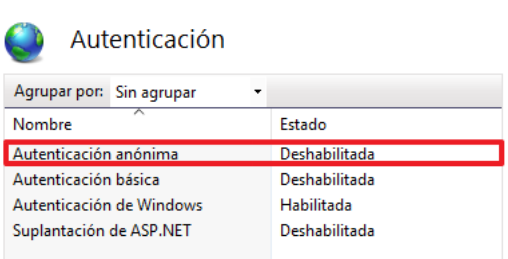
Paso	Descripción
29.	Diríjase hasta la pestaña seguridad. 
30.	A continuación, pulse el botón “Editar”. 
31.	A continuación, seleccione los permisos del que desea establecer para ese sitio web.  **Nota:** Es recomendable dar permiso solo a los usuarios o grupos que deban tener acceso al sitio web evitando que el usuario administrador tenga permiso para prevenir posibles vulnerabilidades.

2.3. AUTENTICACIÓN SITIO WEB

Los métodos de autenticación permitirán limitar el acceso al sitio web a una lista determinada de usuarios (el método habilitado por defecto de los servicios web de IIS es la autenticación anónima), se debe limitar el acceso al contenido web a usuarios anónimos para prevenir posibles ataques.

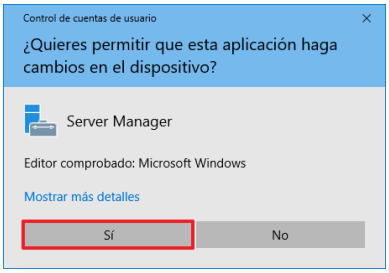
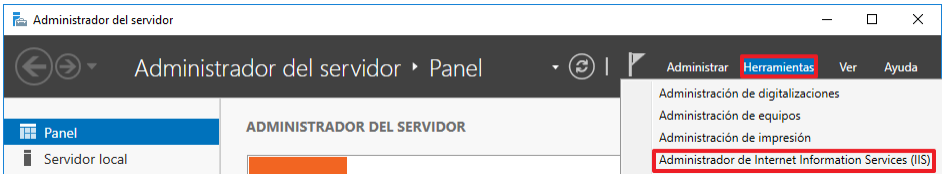
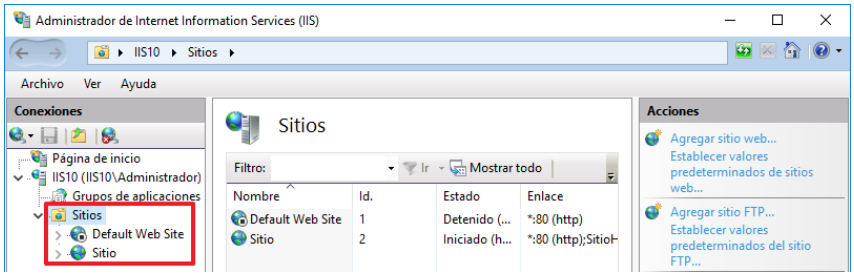
Los siguientes pasos indican cómo deshabilitar la autenticación anónima a nivel de sitio Web.

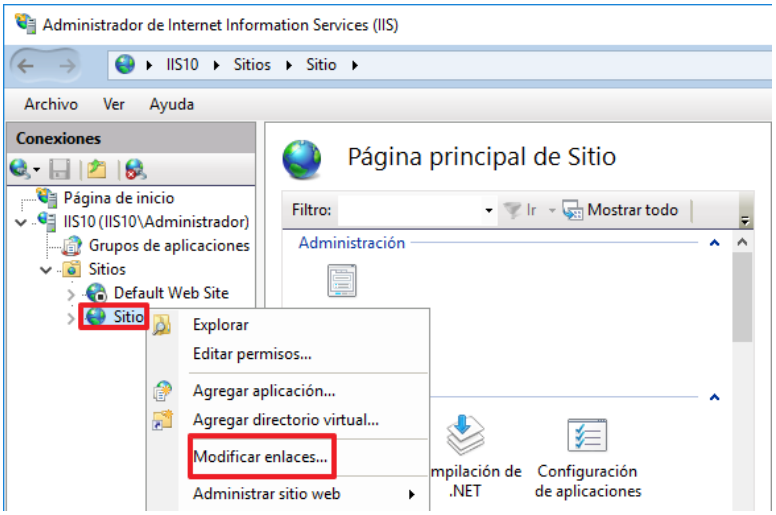
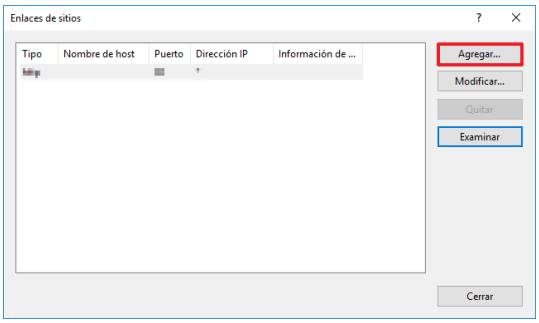
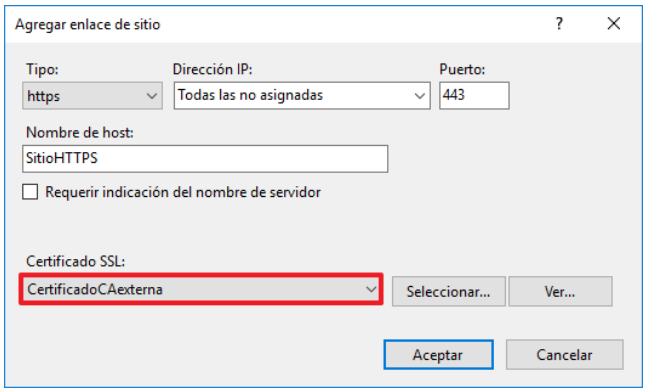
Paso	Descripción
32.	Inicie sesión en el servidor independiente donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
33.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 
34.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione: **“Herramientas → Administrador de Internet Information Services (IIS)”** 

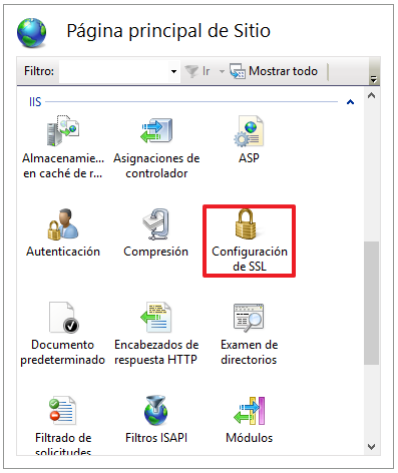
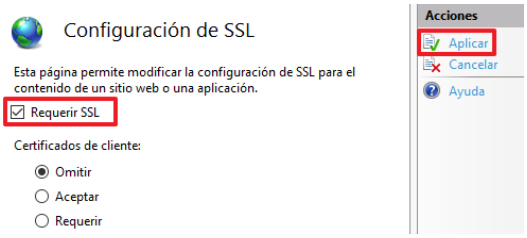
Paso	Descripción
35.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo de “Conexiones” y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.
36.	Seleccione en la página principal del sitio web el icono de “Autenticación”. 
37.	Pulse sobre “Abrir característica” situado en el panel derecho en el menú “Acciones”. 
38.	A continuación, establezca según las características de su organización los métodos de autenticación disponibles. Para ello pulse sobre el método de autenticación que quiere configurar y en el panel derecho seleccione la acción que desea realizar.  **Nota:** Únicamente se usará la autenticación anónima para páginas webs generales en la que solo se muestre contenido y no sea necesaria la autenticación del usuario.

2.4. CERTIFICADOS

IIS 10 faculta el empleo de protocolos seguros para las comunicaciones y los procesos de autenticación usando HTTPS que utiliza un cifrado basado en SSL/TLS para crear un canal cifrado para el tráfico de información sensible. Para lugares públicos es un requisito indispensable en la categoría media del ENS el uso de certificados emitidos por entidades certificadoras de terceros reconocidas, para el caso de sitios internos se recomienda el uso de certificados emitidos por una entidad certificadora interna, está desaconsejado el uso de certificados autofirmados.

Paso	Descripción
39.	Inicie sesión en el servidor independiente donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
40.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar. 
41.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione: **“Herramientas → Administrador de Internet Information Services (IIS)”** 
42.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo de “Conexiones” y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.

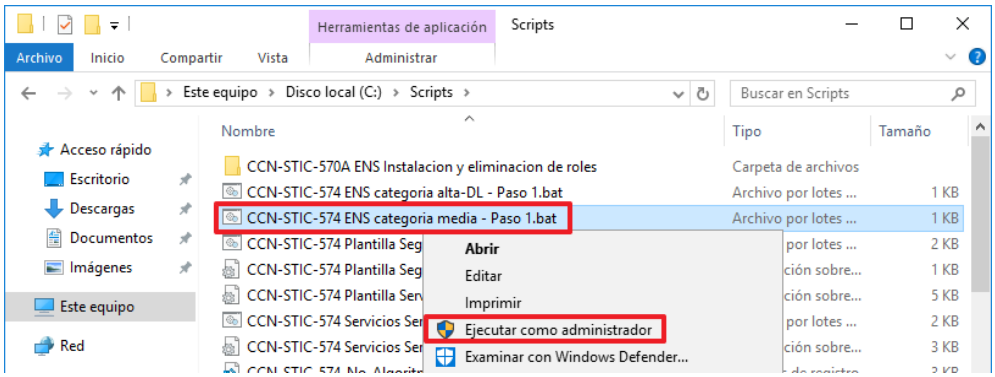
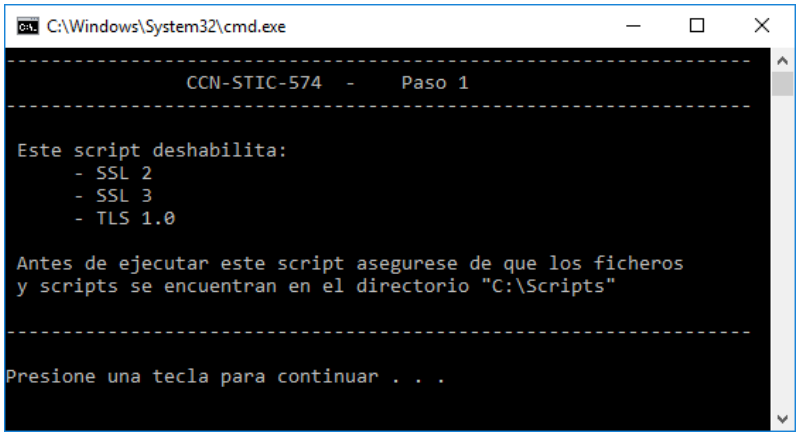
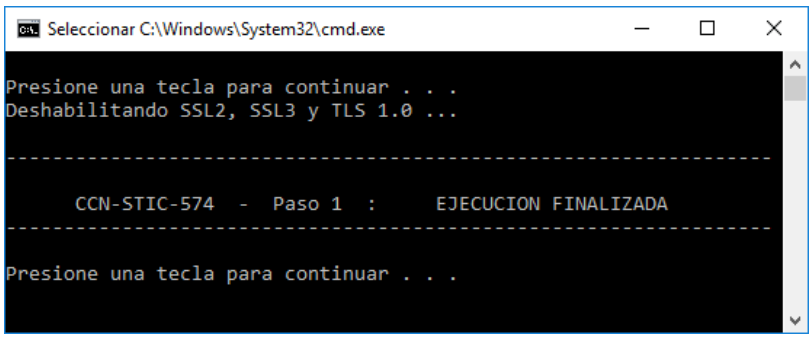
Paso	Descripción
43.	Pulse con el botón derecho sobre el sitio web que quiere modificar y seleccione la opción “Modificar enlaces…”. 
44.	Pulse sobre el botón “Agregar…”. 
45.	Seleccione Tipo: “https”, seleccione Certificado SSL: “CertificadoCAexterna” de una entidad externa y pulse “Aceptar”.  **Nota:** El certificado descrito es uno creado de ejemplo, deberá seleccionar el adecuado para su organización.

Paso	Descripción
46.	A continuación, deberá configurar el sitio web para que los usuarios requieran un certificado propio, para ello pulse sobre en el sitio web que desea configurar, y seleccione “Configuración de SSL”. 
47.	Seleccione la opción de “Requerir SSL” y pulse sobre “Aplicar” para que el sistema guarde los cambios realizados. 
48.	En caso de que usted no cuente con un certificado emitido por una entidad certificadora autorizada debe solicitarlo para cumplir con la categoría media de seguridad del ENS.

2.5. PROTOCOLOS DE TRANSMISIÓN

Con la aplicación del ENS para la categoría media sobre IIS 10 es imprescindible el eliminar el uso de los algoritmos SSL2, SSL3 y TLS1.0, evitando con ello sufrir posibles ataques.

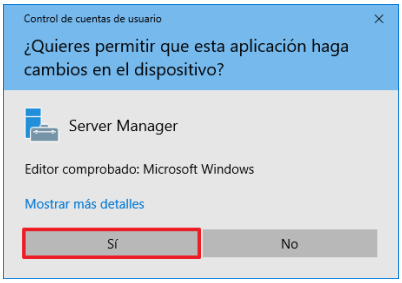
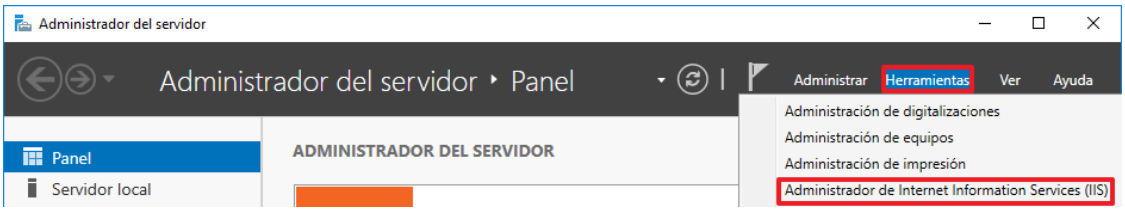
Paso	Descripción
49.	Inicie sesión en el servidor independiente donde tiene instalado el rol de IIS 10.
50.	Si no lo ha realizado anteriormente, cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
51.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.

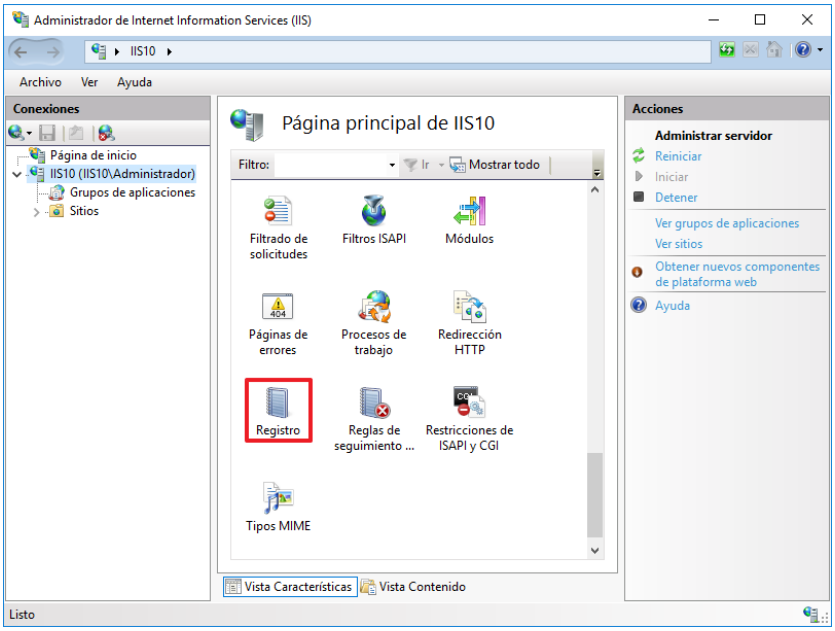
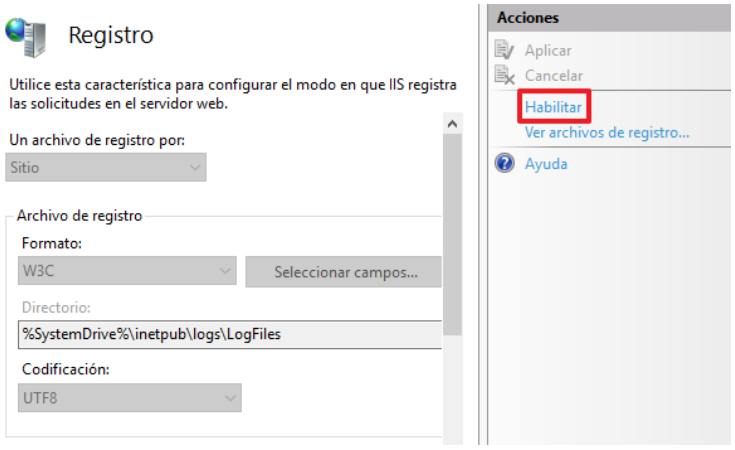
Paso	Descripción
52.	A continuación, debe ejecutar el *script* 1 para deshabilitar los protocolos anteriormente indicados, es necesario realizar esta acción con elevación de privilegios, debe hacer clic con el botón derecho, sobre el fichero denominado "CCN-STIC-574 ENS categoria media – Paso 1.bat" situado en C:\Scripts y haga clic en "Ejecutar como administrador". 
53.	El control de cuentas de usuario le solicitará elevación de permisos para ejecutar el programa, pulse "Si".
54.	Aparecerá la siguiente ventana indicando que va a proceder a deshabilitar los protocolos SSL2, SSL3 y TLS 1.0, pulse cualquier tecla para continuar. 
55.	Una vez finalizada la tarea pulse una tecla para cerrar la ventana. 

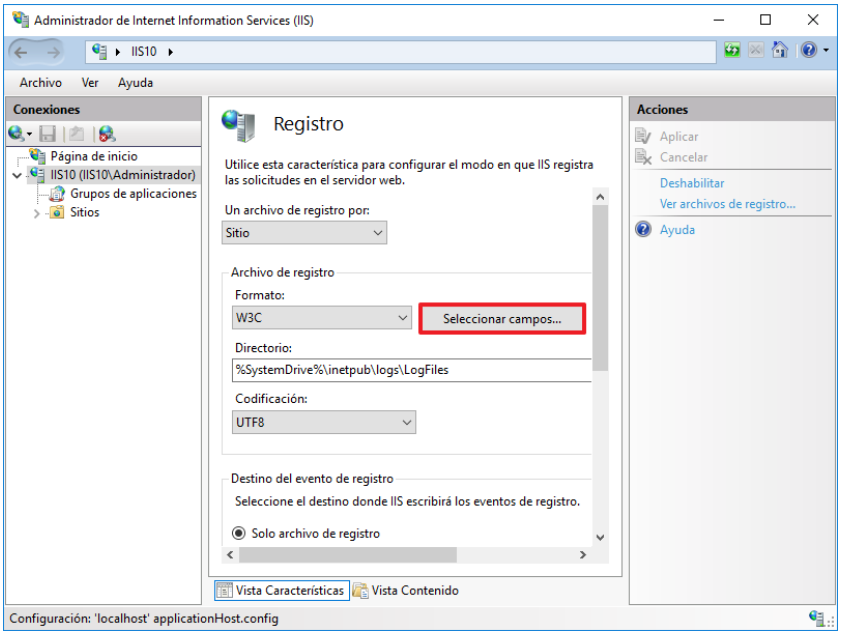
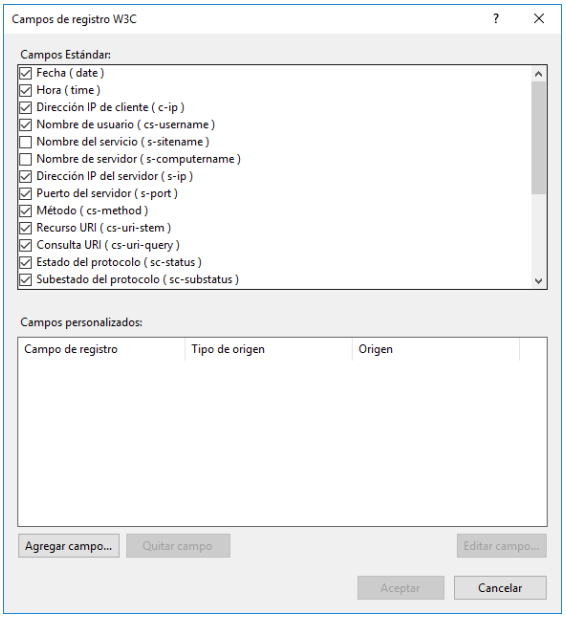
2.6. AUDITORÍA

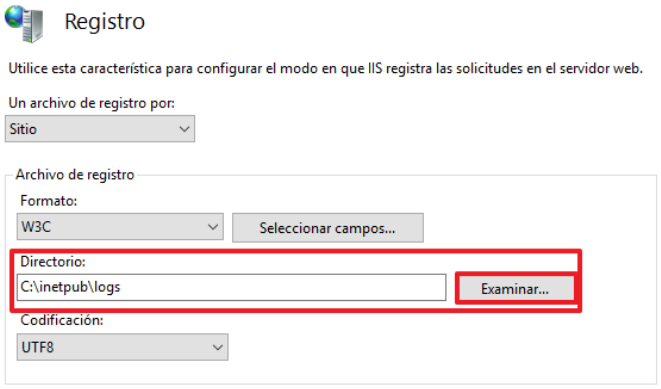
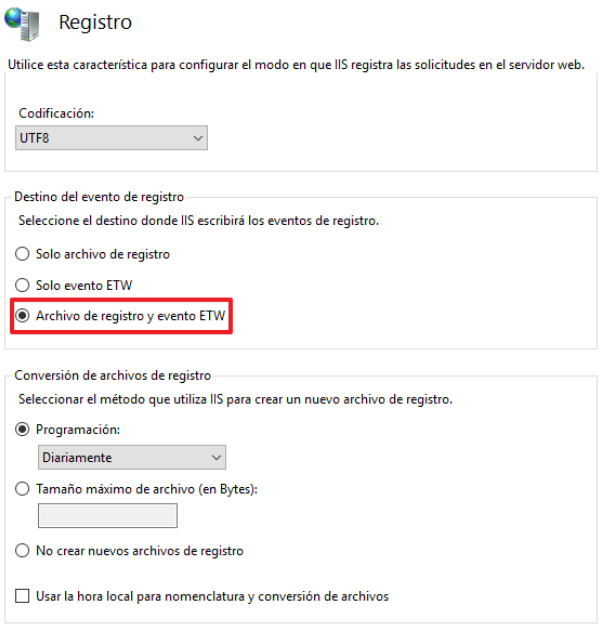
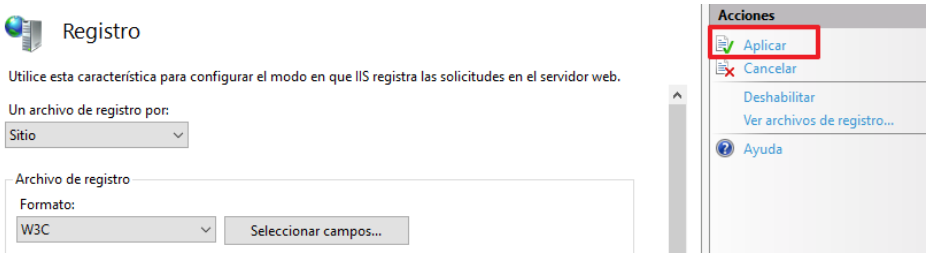
Con la aplicación del ENS para la categoría media sobre IIS 10 quedará registrado el uso del sistema para poder detectar y reaccionar a cualquier fallo accidental o deliberado, quedando registrado en el sistema quien realiza la actividad, cuando y sobre qué información con el fin de detectar anomalías o intentos frustrados de acceso a información no autorizada.

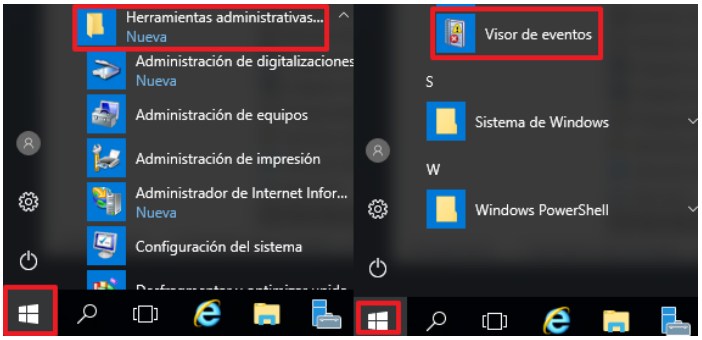
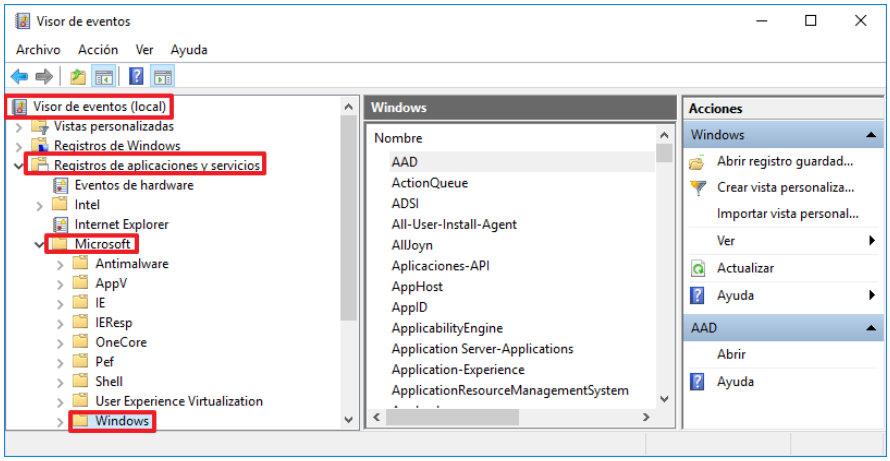
La ubicación de los registros debe ser diferente a la del sistema además de tener limitado el acceso únicamente a los usuarios autorizados.

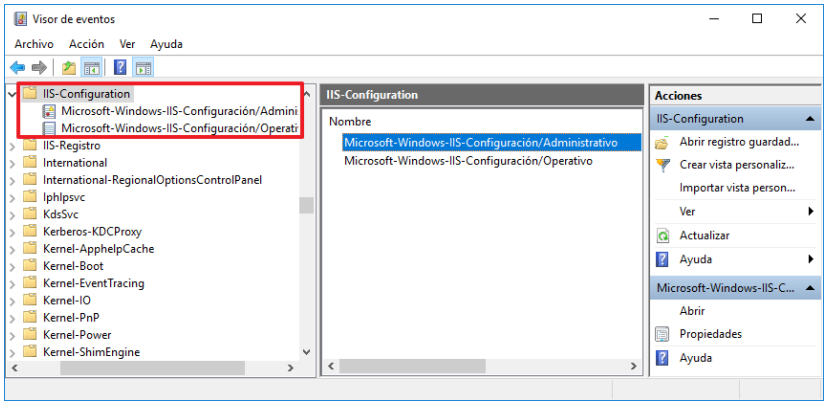
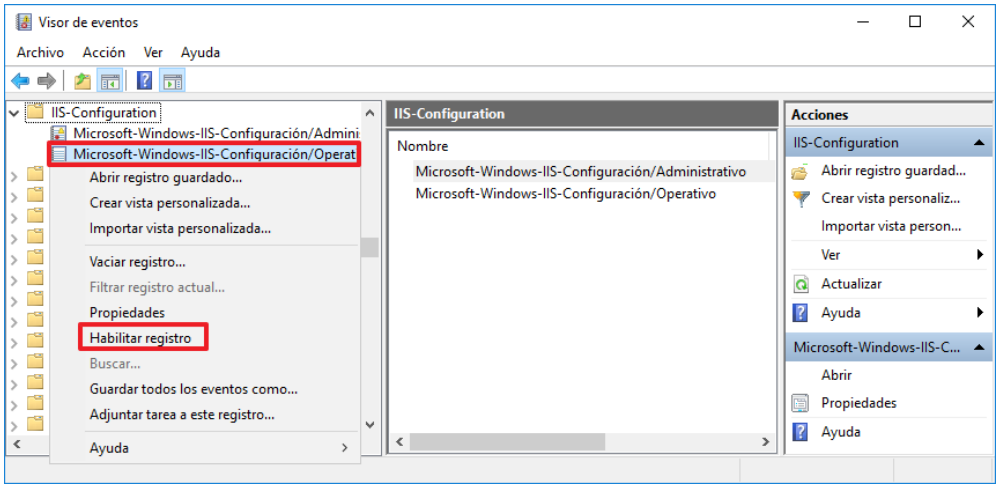
Paso	Descripción
56.	Inicie sesión en el servidor independiente donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
57.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar. 
58.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”** 

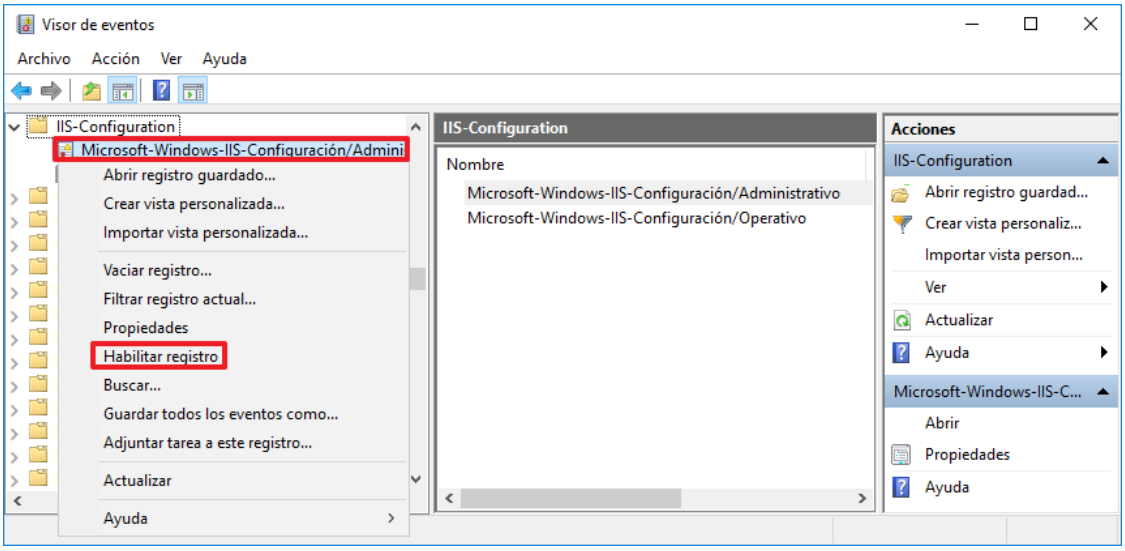
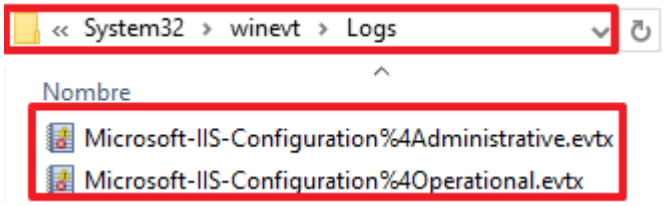
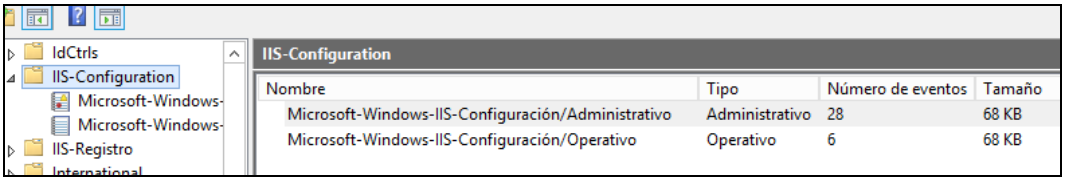
Paso	Descripción
59.	Diríjase al sitio web que desea administrar, a continuación, localice el icono “Registro”, y pulse la acción “Abrir característica” situado en la parte superior derecha de la pantalla para acceder a la configuración del registro. 
60.	Debe habilitar el registro de las solicitudes del servidor IIS 10 para ello, diríjase al menú “Acciones” situado en la parte superior derecha de la pantalla y pulse sobre “Habilitar”. 

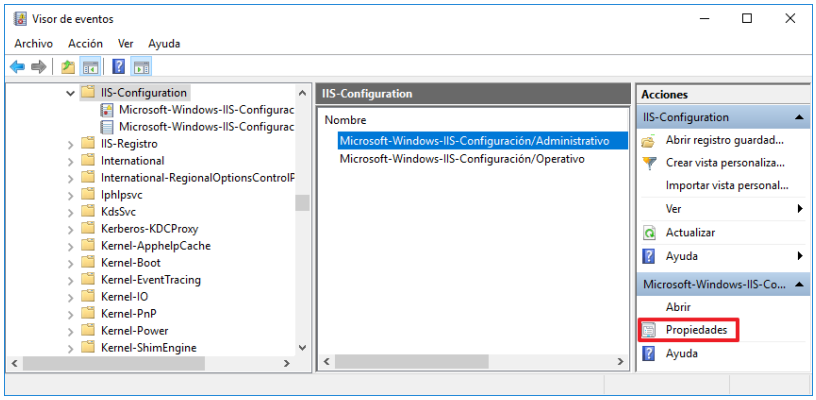
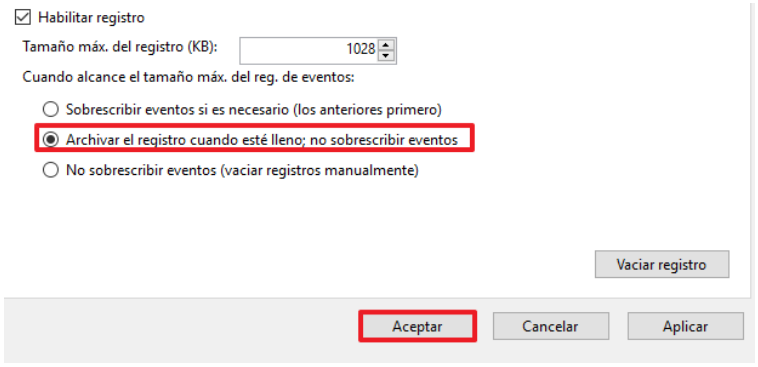
Paso	Descripción
61.	Seleccione los campos que desea registrar, para ello pulse sobre “Seleccionar campos…”. 
62.	Compruebe qué campos se recogerán en el fichero de registro y asegúrese que coincide con sus necesidades. Los valores marcados por defecto suelen ser suficientes, pero no descarte marcar otros. 

Paso	Descripción
63.	A continuación, seleccione el directorio donde se van a guardar los registros, por seguridad es recomendable realizarlo en una unidad diferente a la de la instalación del sistema operativo. 
64.	A continuación, deberá seleccionar el destino del evento, seleccione, “Archivo de registro y evento ETW”. 
65.	Una vez realizados los cambios deberá guardarlos, para ello pulse “Aplicar” situado en el menú “Acciones” en la parte superior izquierda de la pantalla. 

Paso	Descripción
66.	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.
67.	Debe abrir el Visor de eventos, ejecutándolo como administrador, como en ocasiones anteriores: "**Menú inicio → Herramientas administrativas→ Visor de eventos**".  **Nota:** El sistema solicitará elevación de privilegios para completar la acción.
68.	Seleccione en el árbol "**Visor de eventos → Registro de aplicaciones y servicios → Microsoft → Windows**". 

Paso	Descripción
69.	Desplácese hacia abajo, podrá observar que Microsoft Windows Server 2016 dispone de dos grupos de registros para IIS, dentro del de configuración se encuentran: administrativo y operaciones. Es necesario activar ambos, según se le indica a continuación. 
70.	Sitúese sobre el registro operativo, abra el menú contextual con el botón derecho del ratón y seleccione “Habilitar registro”.  **Nota:** Cualquier acción operativa sobre el servidor quedará recogida a partir de ahora.

Paso	Descripción
71.	Haga lo mismo para el registro “Administrativo”. 
72.	Los registros se habrán creado en el disco duro, en la partición del sistema operativo (habitualmente la C:) y en la ruta **%SystemRoot%\System32\winevt\Logs**, con los nombres: – Microsoft IIS-Configuration%4Operational.evtx – Microsoft IIS-Configuration%4Administrative.evtx  **Nota:** La variable %SystemRoot% corresponde a C:\Windows\System32 en las configuraciones habituales de las guías.
73.	Los ficheros se crean con tamaño cero pero se empezarán a poblar automáticamente desde este momento. 

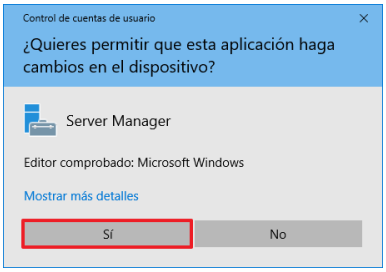
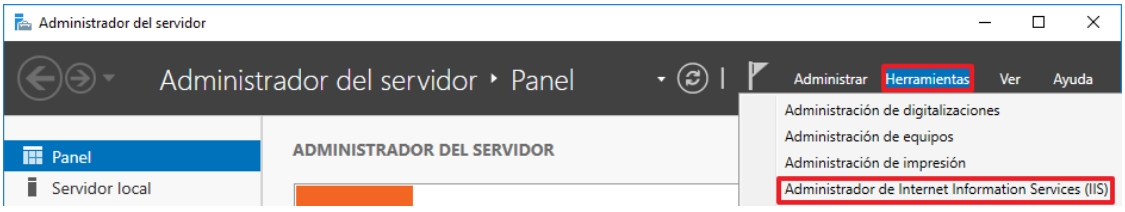
Paso	Descripción
74.	Para acceder a las propiedades de los ficheros, seleccione un fichero y pulse sobre la opción “Propiedades” del menú “Acciones”.  **Nota:** Tenga en cuenta que el registro administrativo se llenará, en condiciones normales, antes que el operacional.
75.	Para evitar, que una vez completado 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”.
76.	Con la configuración dejada, 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.

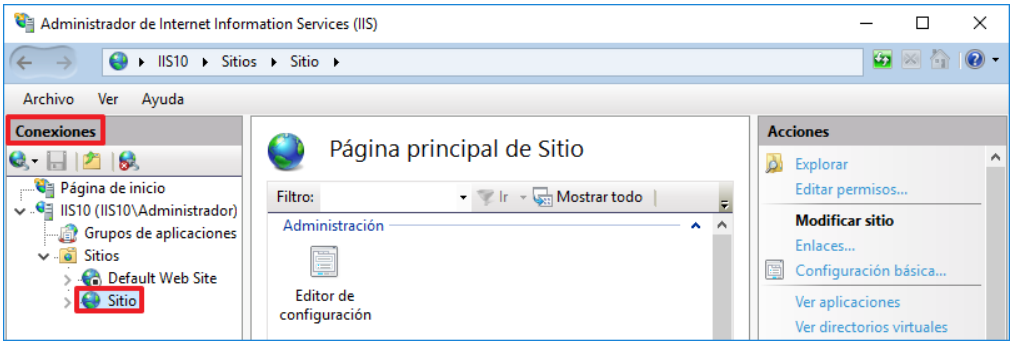
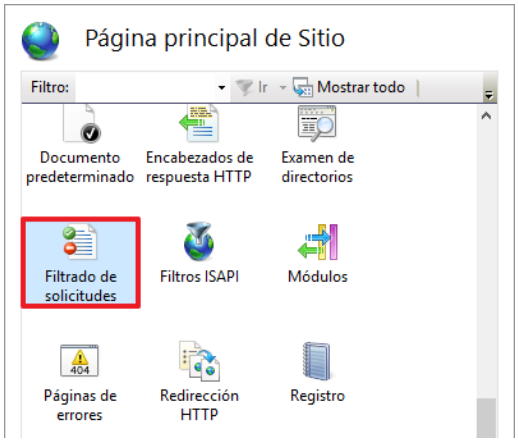
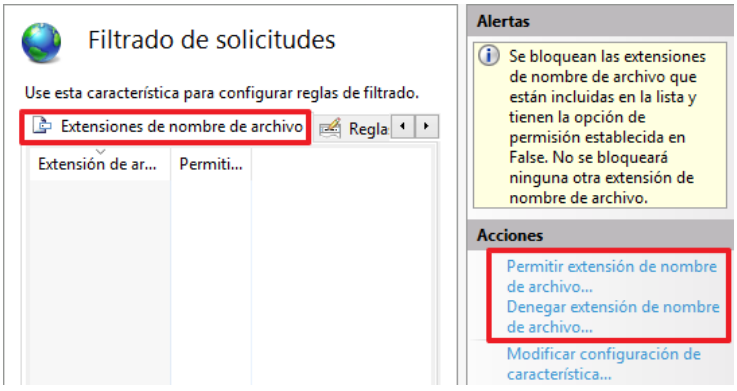
2.7. FILTRADO DE SOLICITUDES

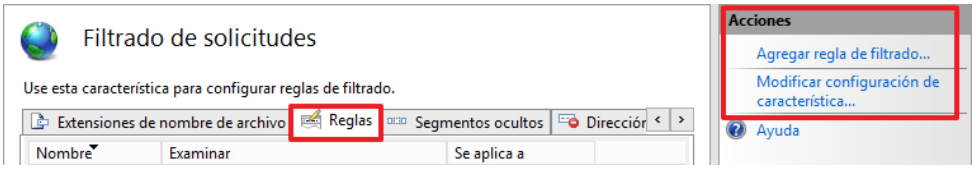
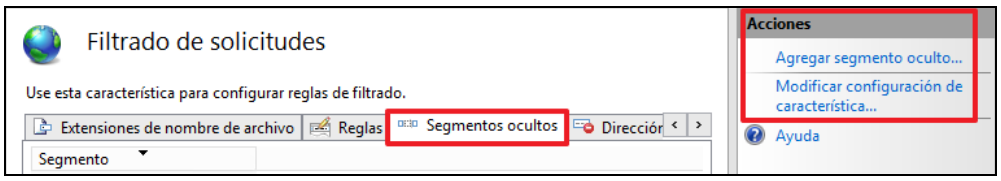
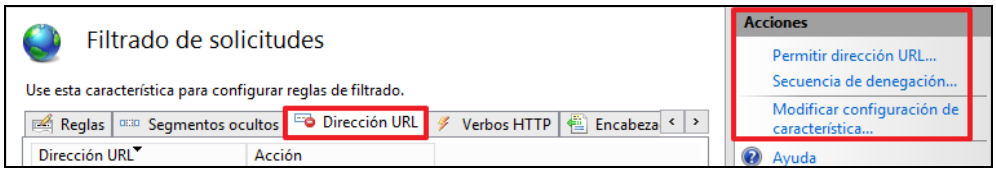
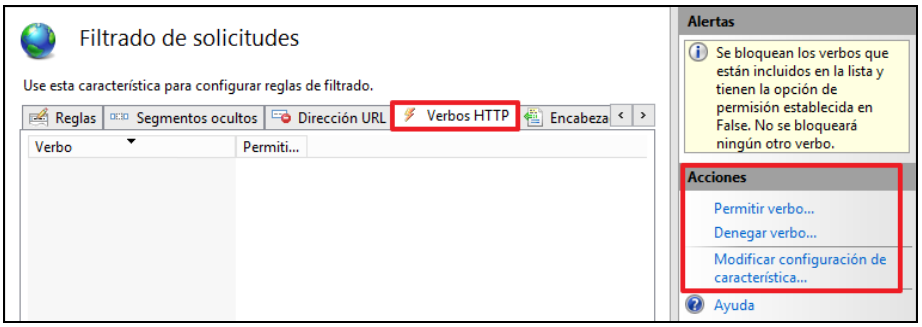
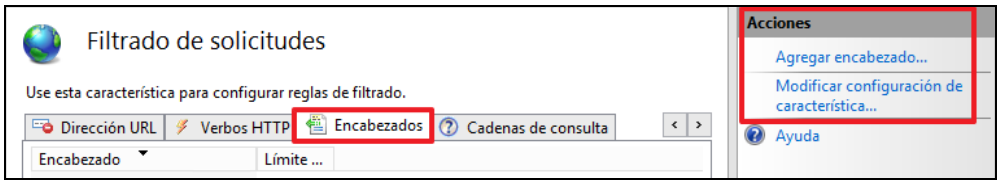
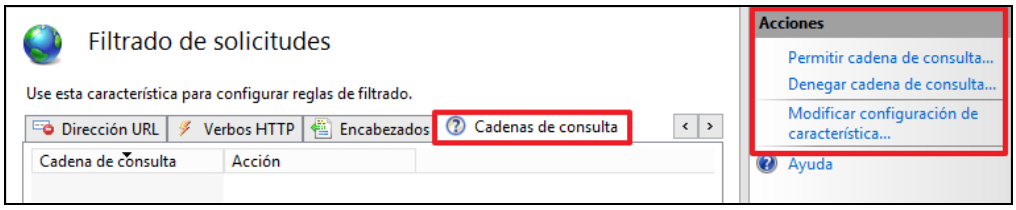
El siguiente paso define el procedimiento para la configuración del filtro de solicitudes el cual se encarga de analizar todas las solicitudes que entran en el servidor web y las filtra basándose en reglas establecidas previamente.

La mayoría de los ataques malintencionados comparten características comunes, como direcciones URL muy largas o solicitudes de una acción inusual, es por ello que filtrando las solicitudes se puede reducir el impacto de este tipo de ataques.

Cada organización debe determinar que extensiones son las específicamente necesarias para la funcionalidad del sitio web que tiene alojado y deberá configurar el filtro para soportar únicamente las extensiones exclusivamente necesarias.

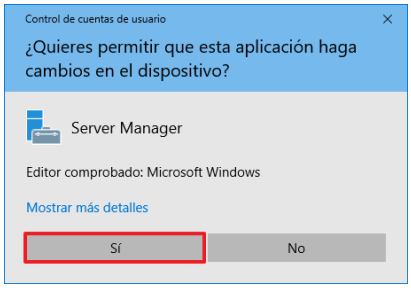
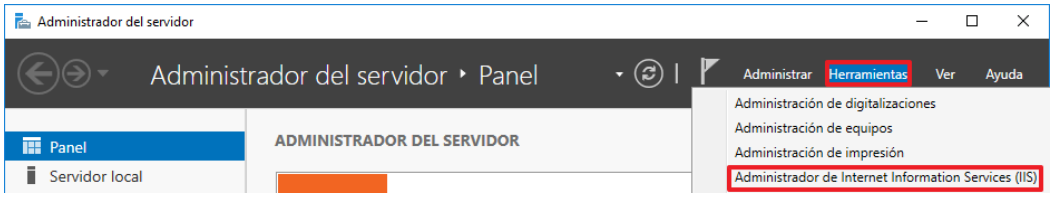
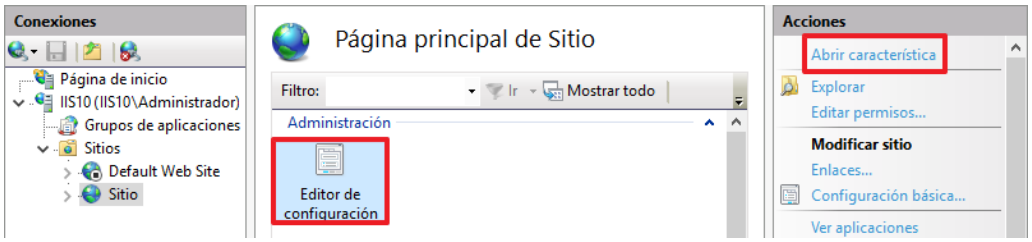
Paso	Descripción
77.	Inicie sesión en el servidor independiente donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
78.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 
79.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione: **“Herramientas → Administrador de Internet Information Services (IIS)”** 

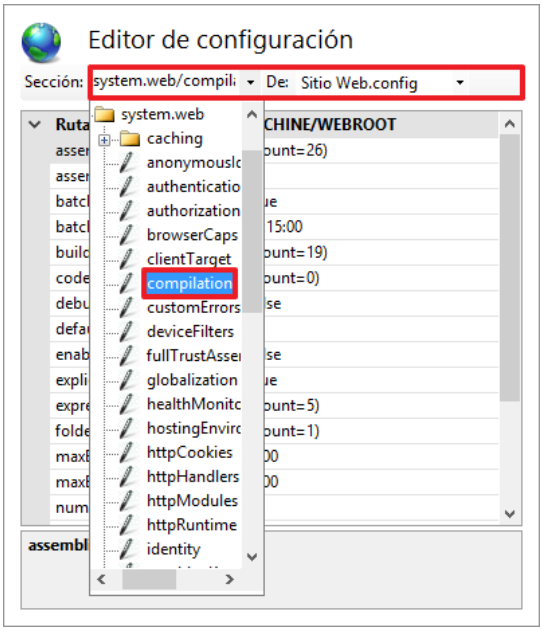
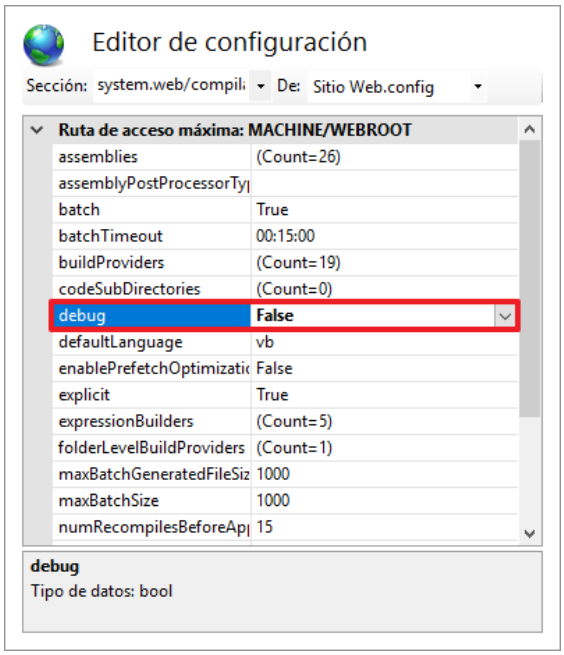
Paso	Descripción
80.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo de “Conexiones” y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.
81.	Seleccione en la página principal del sitio web el icono “Filtrado de solicitudes” y pulse sobre “Abrir característica” sitiado en el menú acciones del panel superior derecho de la pantalla. 
82.	A continuación, en la pestaña “Extensiones de nombre de archivo” puede permitir o denegar extensiones. 

Paso	Descripción
83.	En la siguiente pestaña puede agregar o modificar reglas de filtrado. 
84.	En la siguiente pestaña puede agregar o modificar segmentos ocultos. 
85.	En la siguiente pestaña puede permitir, denegar o modificar direcciones URL. 
86.	En la siguiente pestaña puede permitir, denegar o modificar Verbos. 
87.	En la siguiente pestaña puede agregar o modificar encabezados. 
88.	En la siguiente pestaña puede permitir, denegar o modificar cadenas de consulta. 

2.8. DESHABILITAR MODOS DE DEPURACIÓN

El siguiente paso define el procedimiento para la modificación del fichero web.config para inhabilitar el modo de depuración de una aplicación en entornos de producción, evitando con ello posibles fisuras de seguridad.

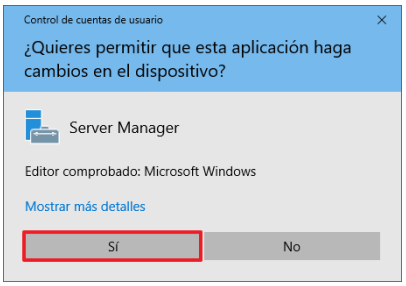
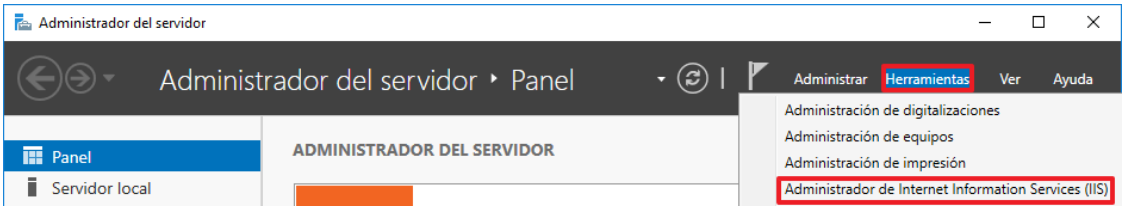
Paso	Descripción
89.	Inicie sesión en el servidor independiente donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
90.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 
91.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione: **“Herramientas → Administrador de Internet Information Services (IIS)”** 
92.	Localice el sitio web que desea configurar y seleccione “Editor de configuración”, a continuación, pulse en el menú “Acciones” la opción “Abrir característica” situado en la parte superior derecha de la pantalla para abrir el editor de configuración. 

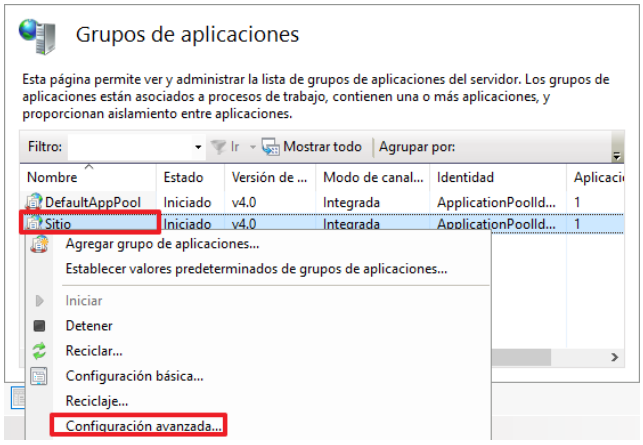
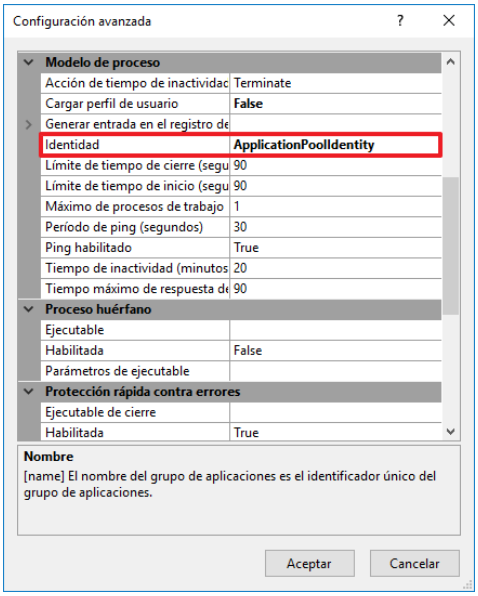
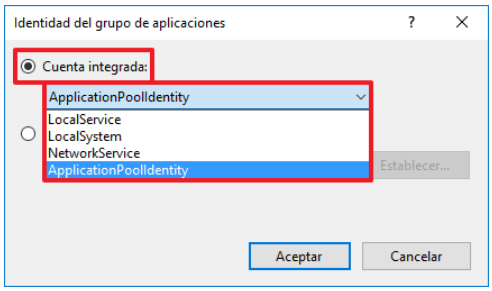
Paso	Descripción
93.	Navegue en “Sección” hasta “system.web/compilation”. 
94.	Localice la opción “Debug”, abra el desplegable y seleccione “False”. 

2.9. IDENTIDADES DEL GRUPO DE APLICACIONES

El siguiente paso define el procedimiento para la modificación de las identidades de una aplicación las cuales deben modificarse con la aplicación del ENS para la categoría media sobre IIS 10 y evitando el uso de identidades de servicio integradas tales como servicio local o sistema local.

Para una mayor seguridad los grupos de aplicaciones deben ejecutarse bajo la identidad del grupo cuando se crea el grupo de aplicaciones, el valor predeterminado y más seguro es "ApplicationPoolIdentity". El uso de una cuenta personalizada es aceptable, pero debe asegurarse de usar una cuenta diferente para cada grupo de aplicaciones.

Paso	Descripción
95.	Inicie sesión en el servidor independiente donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
96.	El sistema solicitará elevación de privilegios. Pulse sobre el botón "Sí" para confirmar la operación. 
97.	Inicie la herramienta "Administrador de Internet Information Services (IIS)". Para ello, pulse sobre el menú superior de la derecha de la herramienta "Administrador del servidor" y seleccione: **"Herramientas → Administrador de Internet Information Services (IIS)"** 
98.	Despliegue el servidor y seleccione la opción "Grupos de aplicaciones". 

Paso	Descripción
99.	A continuación, seleccione la aplicación que desea configurar y haga clic botón derecho sobre ella y pulse “Configuración avanzada…”. 
100.	Localice la opción “Identidad” dentro de “Modelo de proceso”. 
101.	Seleccione la opción que más se adecue a sus necesidades y pulse aceptar. 

2.10. LIMPIEZA DE METADATOS

Se ha de tener en consideración que en un servidor web se pueden alojar documentos que pueden contener información oculta en los metadatos los cuales contienen información que permite catalogar, ordenar y clasificar nuestros archivos, por lo que pueden ser un riesgo de seguridad para nuestra organización, por lo que hay que tener especial atención en la limpieza de los metadatos de los documentos que se alojan en el servidor web por ello antes de alojar un fichero en el servidor web se ha debido de realizar el procedimiento indicado en MP. INFO. 6. LIMPIEZA DE DOCUMENTOS.

En el proceso de limpieza se ha de tener en consideración que se retiraran todos los datos de los documentos además de la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, con la excepción de la información pertinente para el receptor del documento.

2.11. SOLUCIONES WAF (WEB APLICATION FIREWALL)

Un servidor web puede alojar aplicaciones por lo que es importante un control exhaustivo de estas por ello se han de emplear uno de los elementos principales en la protección de entornos de aplicaciones Web que son los cortafuegos (firewalls) de aplicaciones Web, también conocidos como WAF, Web Application Firewall.

El WAF se encargará de proteger los servidores de aplicaciones web de determinados ataques específicos en Internet además de controlar las transacciones al servidor web de nuestra organización.

Este sistema nos permite evitar probables ataques como:

a) “Cross-site scripting” que consiste en la inclusión de código script malicioso en el cliente que consulta el servidor web.

b) “SQL injection” que consiste en introducir un código SQL que vulnere la Base de Datos de nuestro servidor.

c) “Denial-of-service” que consiste en que el servidor de aplicación sea incapaz de servir peticiones correctas de usuarios.

Algunos sistemas WAF existentes en el mercado también monitorizan las respuestas del servidor, por ejemplo, si en una respuesta, que el servidor web envía al usuario se detectan cadenas que pueden ser identificadas como cuentas bancarias, el WAF lo puede detectar como un posible ataque y denegar la respuesta.

3. GESTIÓN DE ROLES Y/O CARACTERÍSTICAS DEL SISTEMA

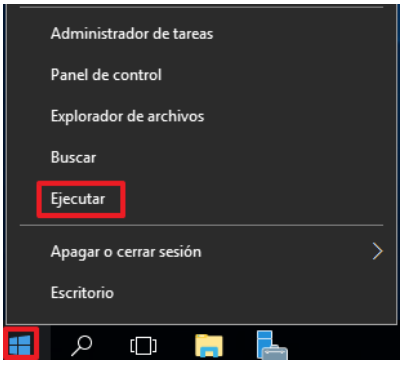
Estos paso a paso se deberán aplicar para instalar o desinstalar roles y/o características implementadas en un servidor independiente, que le sea de aplicación la guía de securización “CCN-STIC-570B - Implementación del ENS en Microsoft Windows Server 2016 Servidor independiente” a partir de la categoría media del ENS.

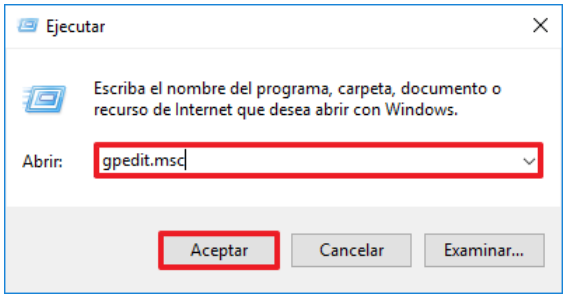
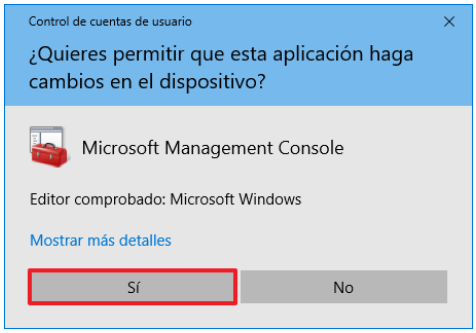
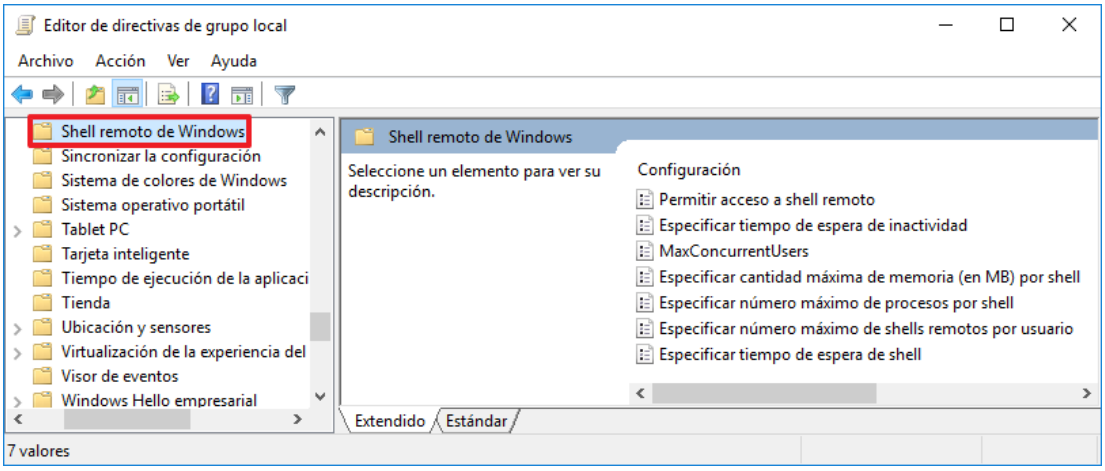
3.1. PREPARACIÓN DEL SERVIDOR INDEPENDIENTE

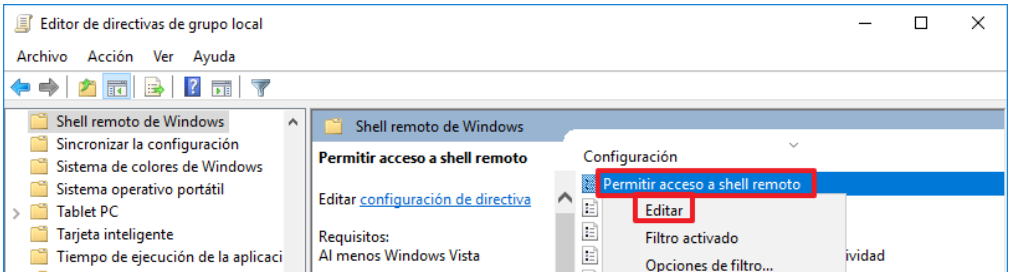
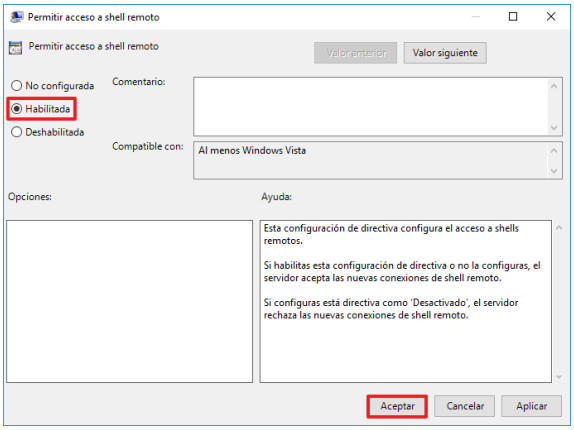
Para instalar o eliminar un rol y/o característica será necesario la modificación de una directiva de grupo.

Los pasos que se describen a continuación se realizarán en el servidor independiente que se está securizando.

Nota: Recuerde que una vez instalados o eliminados los roles y/o características necesarias deberá aplicar el paso "3.4 DESHABILITACIÓN DE UNA DIRECTIVA DE GRUPO LOCAL".

Paso	Descripción
102.	Inicie sesión en el servidor independiente donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador local del equipo.
103.	Inicie el "Editor de directicas de grupo local" para ello pulse sobre el botón de inicio con clic derecho. 
104.	Seleccione la opción del menú contextual "Ejecutar". 

Paso	Descripción
105.	A continuación, escriba el comando “gpedit.msc” y pulse el botón “Aceptar”. 
106.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
107.	Despliegue la política y sitúese en la siguiente ruta. **“Directiva Equipo Local → Configuración del equipo → Plantillas administrativas → Componentes de Windows → Shell remoto de Windows”**. 

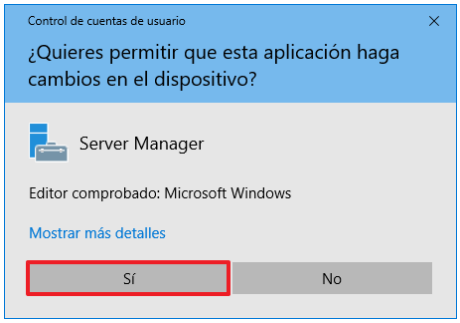
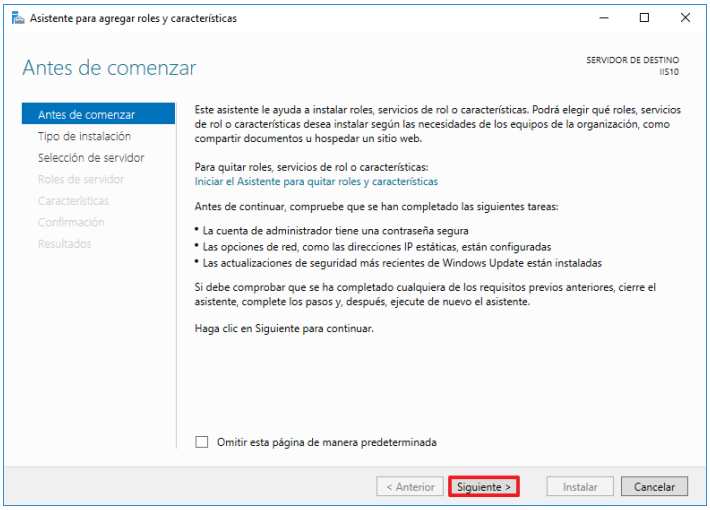
Paso	Descripción
108.	Seleccione la opción “Permitir acceso a Shell remoto”. A continuación, pulse botón derecho y seleccione la opción del menú contextual “Editar”. 
109.	A continuación, marque la opción “Habilitada” y pulse “Aceptar”. 
110.	Para finalizar cierre el “Editor de directivas de grupo local”

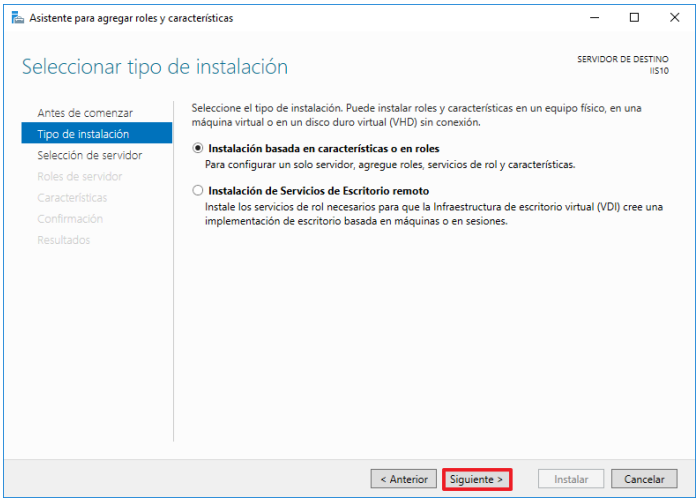
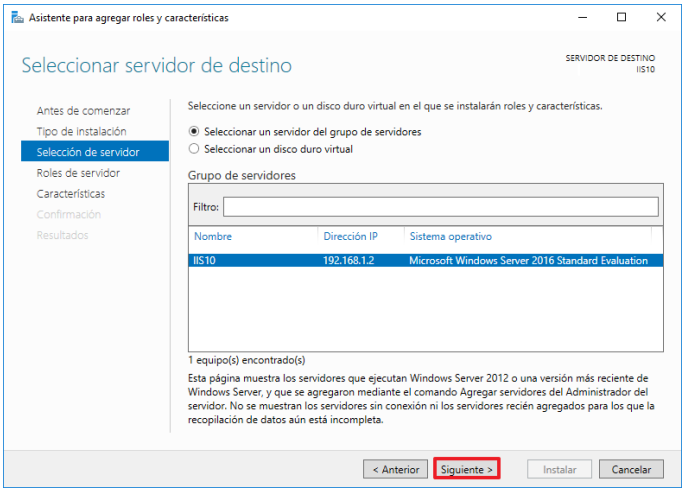
3.2. INSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS

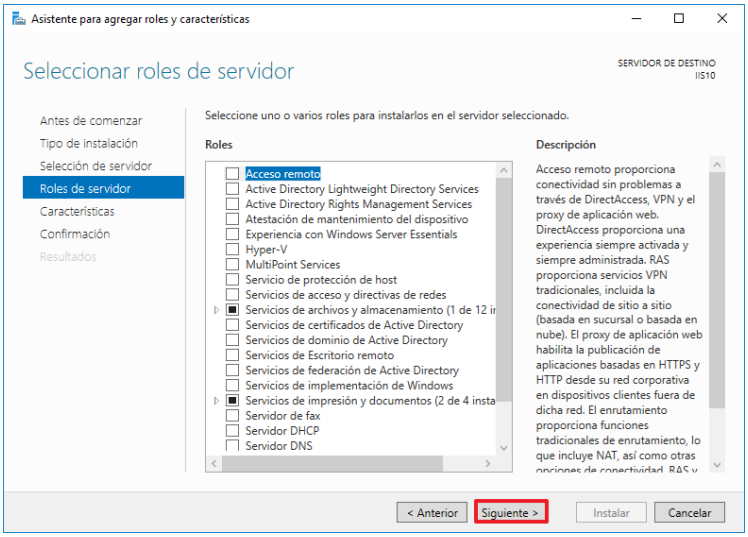
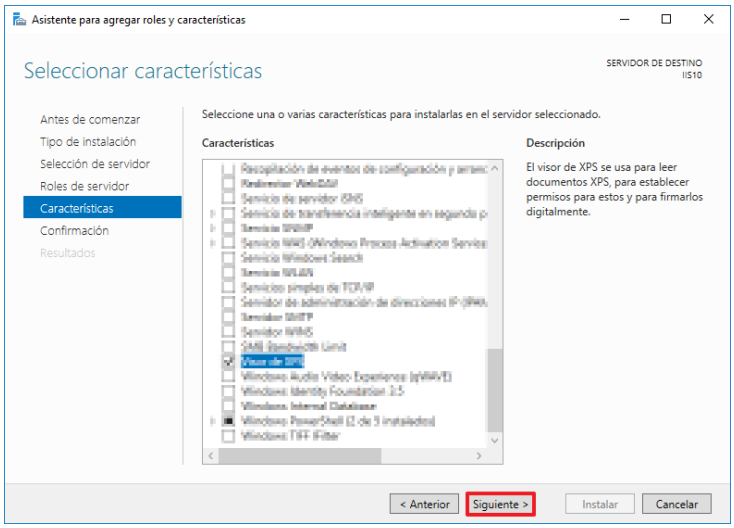
Los pasos que se describen a continuación se realizarán en el servidor independiente que se está securizando.

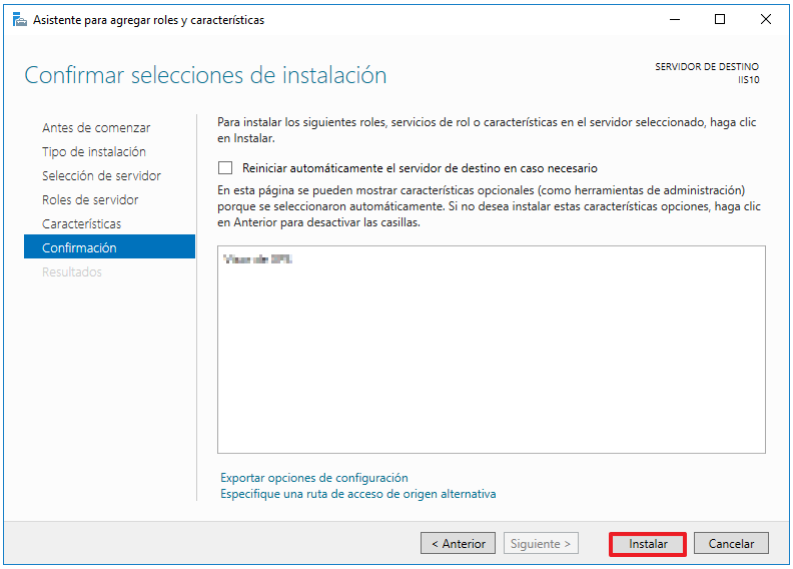
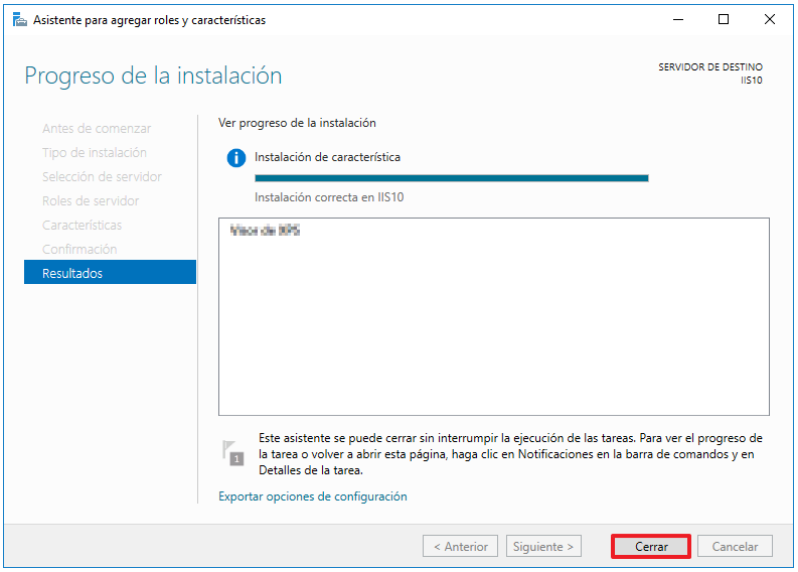
Nota: Para continuar este paso a paso debe haber aplicado previamente el punto “3.1 PREPARACIÓN DEL SERVIDOR INDEPENDIENTE”.

Paso	Descripción
111.	Inicie sesión en el servidor independiente donde vaya a instalar un rol y/o característica.  **Nota:** Inicie sesión con una cuenta que sea administrador local del equipo.

Paso	Descripción
112.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
113.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
114.	A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Agregar roles y características”. 
115.	Comenzará el asistente para agregar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 

Paso	Descripción
116.	Seleccione el tipo de instalación, “Instalación basada en características o roles” y pulse “Siguiente >” para continuar. 
117.	Seleccione el servidor sobre el cual desea instalar un rol o una característica, y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “IIS10”.

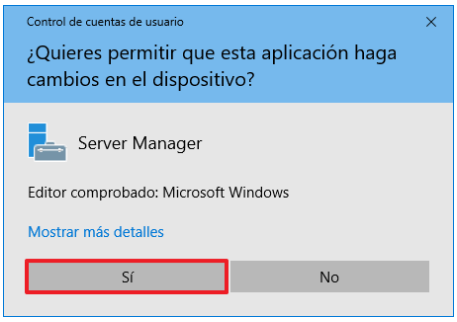
Paso	Descripción
118.	En la siguiente ventana, seleccione los roles que desee instalar en el sistema y pulse “Siguiente >”. 
119.	A continuación, en la siguiente ventana podrá seleccionar las características que desee instalar en el sistema. Seleccione aquellas que desee instalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se instala la característica como prueba, deberá adaptar este paso a los requerimientos de su organización.

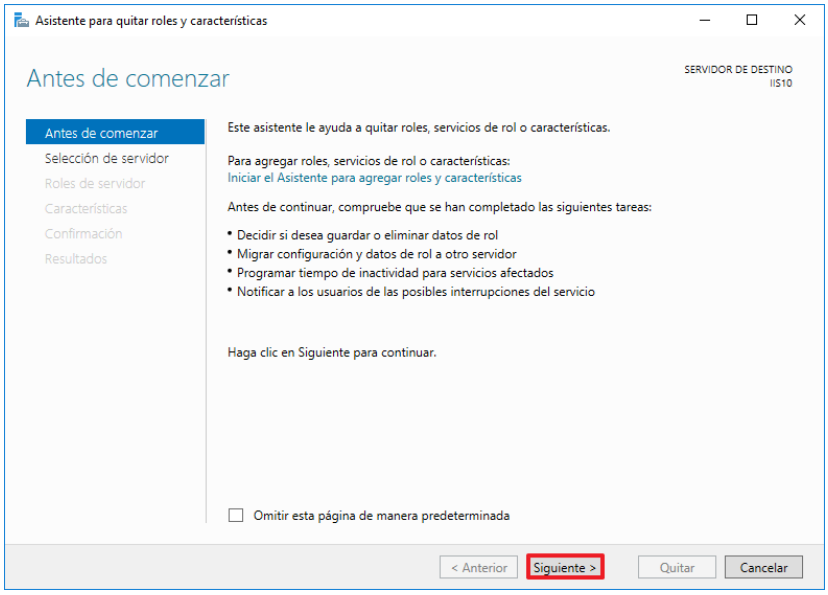
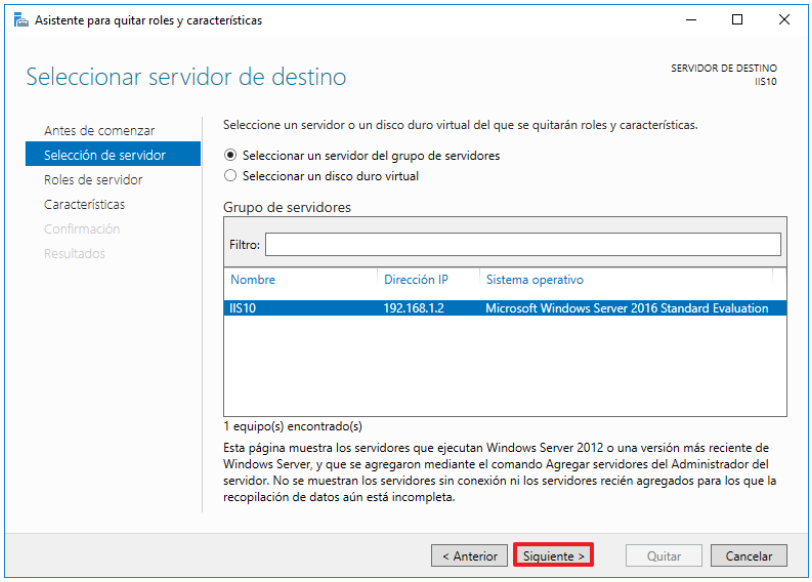
Paso	Descripción
120.	En la ventana “Confirmación” pulse “Instalar” para iniciar el proceso. 
121.	Una vez finalizado el proceso de instalación, pulse sobre “Cerrar” para finalizar la instalación.  **Nota:** En caso de ser necesario, el servidor requerirá un reinicio para finalizar la instalación de roles y características.
122.	Una vez finalizada la instalación de roles y/o características, deberá aplicar el siguiente paso “3.4 DESHABILITACIÓN DE UNA DIRECTIVA DE GRUPO LOCAL”.

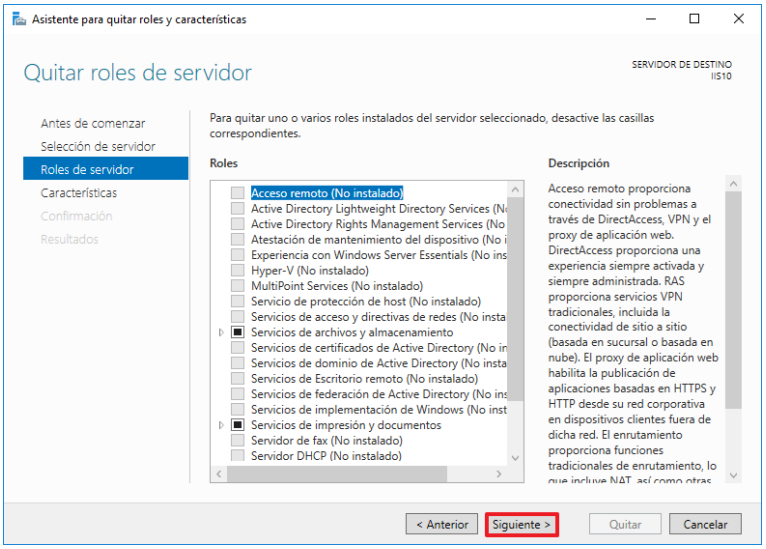
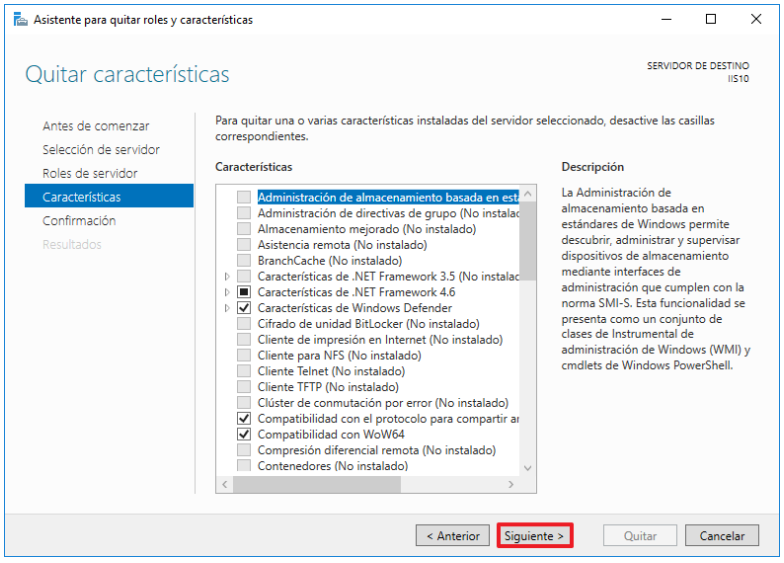
3.3. DESINSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS

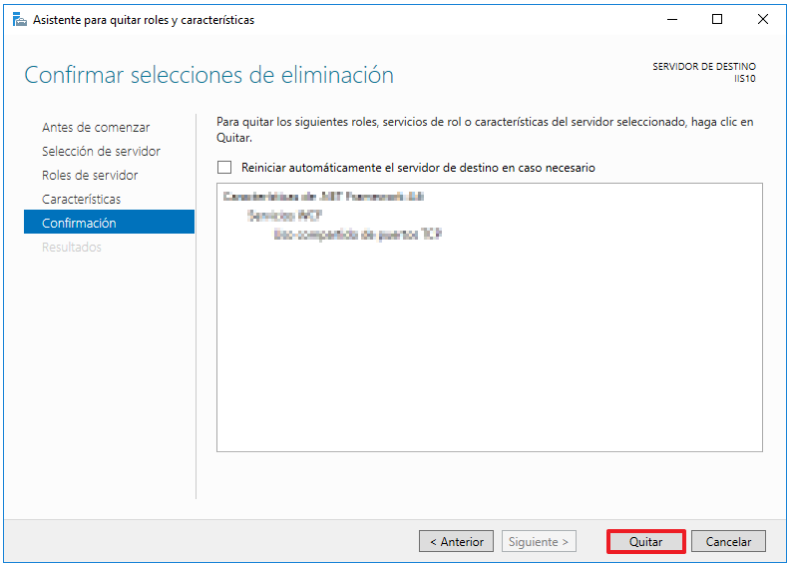
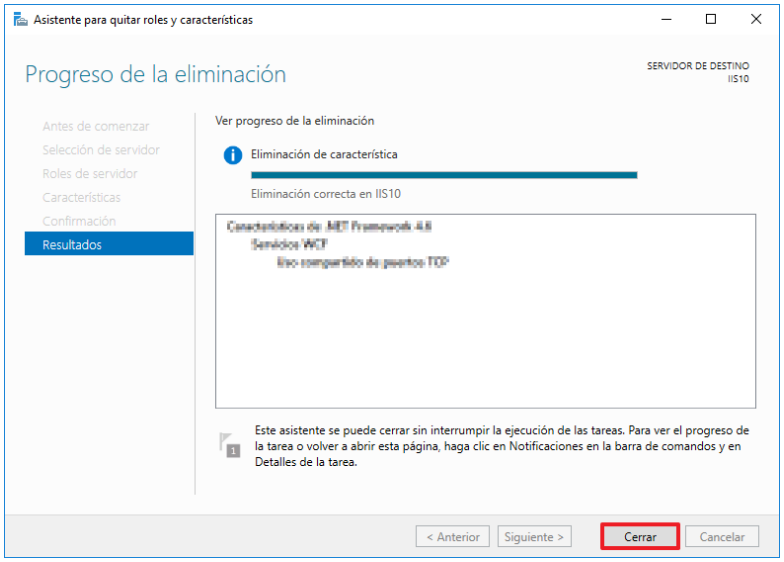
Los pasos que se describen a continuación se realizarán en el servidor independiente que se está securizando.

Nota: Para continuar este paso a paso debe haber aplicado previamente el punto "3.1 PREPARACIÓN DEL SERVIDOR INDEPENDIENTE".

Paso	Descripción
123.	Inicie sesión en el servidor independiente donde vaya a eliminar un rol y/o característica.  **Nota:** Inicie sesión con una cuenta que sea administrador local del equipo.
124.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
125.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
126.	A continuación, pulse sobre el botón "Administrar" y seleccione la opción "Quitar roles y funciones". 

Paso	Descripción
127.	Comenzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 
128.	Seleccione el servidor sobre el cual desea eliminar un rol o una característica y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “IIS10”.

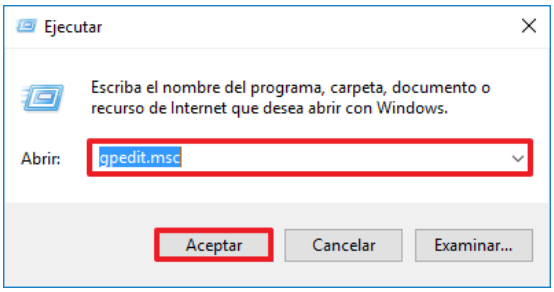
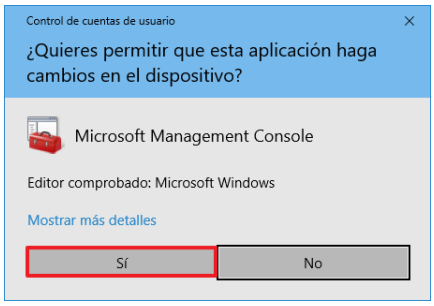
Paso	Descripción
129.	En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Seleccione aquellos que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo no se desinstala ningún rol, deberá adaptar este paso a los requerimientos de su organización.
130.	A continuación, en la siguiente ventana podrá seleccionar las características que desee desinstalar del sistema. Desmarque aquellas que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se desinstala una característica de prueba, deberá adaptar este paso a los requerimientos de su organización.

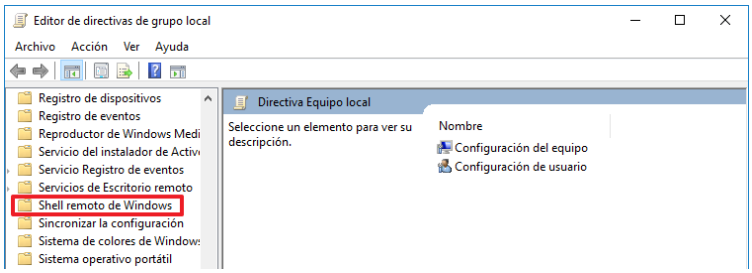
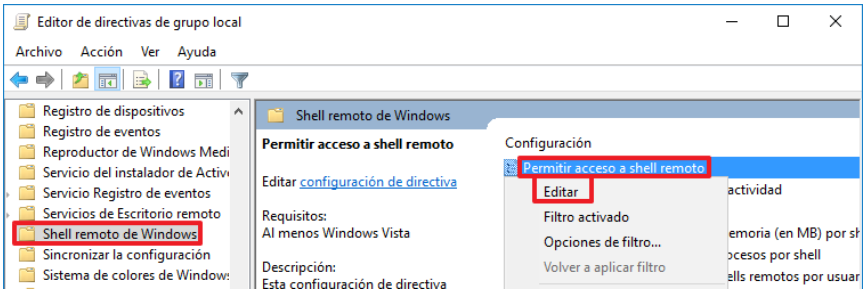
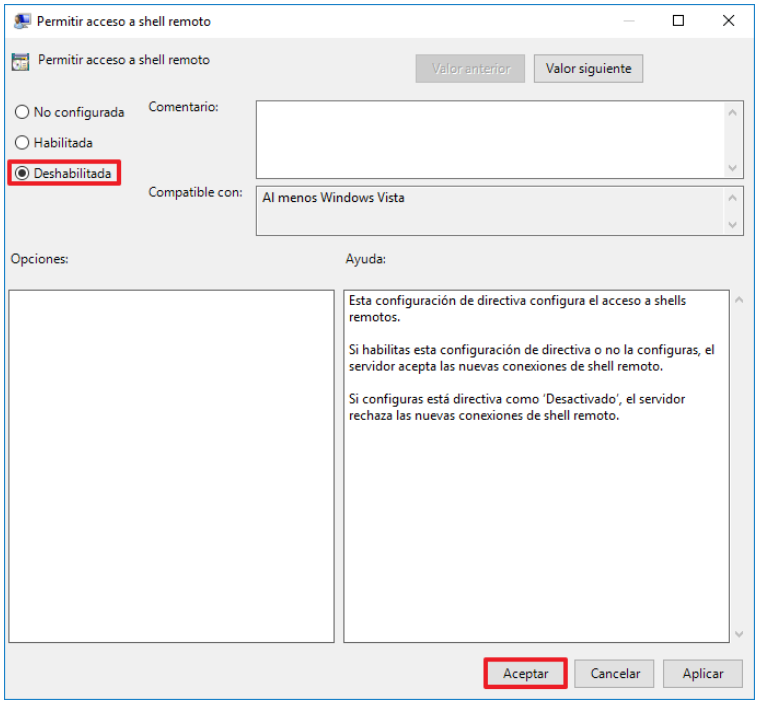
Paso	Descripción
131.	En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso. 
132.	Una vez finalizado el proceso de desinstalación, pulse sobre “Cerrar” para finalizar la desinstalación.  **Nota:** En caso de ser necesario el servidor requerirá un reinicio para finalizar la desinstalación de roles y características.
133.	Una vez finalizada la desinstalación de roles y/o características, deberá aplicar el siguiente paso “3.4 DESHABILITACIÓN DE UNA DIRECTIVA DE GRUPO LOCAL”.

3.4. DESHABILITACIÓN DE UNA DIRECTIVA DE GRUPO LOCAL

Para deshabilitar la directiva de grupo local modificada en el paso “3.1 PREPARACIÓN DEL SERVIDOR INDEPENDIENTE” deberá implementar el siguiente paso a paso.

Los pasos que se describen a continuación se realizarán en el servidor independiente que se está securizando.

Paso	Descripción
134.	Inicie sesión en el servidor donde se va a aplicar la seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador local del equipo.
135.	Inicie el "Editor de directicas de grupo local" para ello pulse botón sobre el botón correspondiente en la barra de tareas. 
136.	Seleccione la opción del menú contextual "Ejecutar" pulsando "Windows+R".
137.	A continuación, escriba el comando "gpedit.msc" y pulse el botón "Aceptar". 
138.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Si". 

Paso	Descripción
139.	Despliegue la política y sitúese en la siguiente ruta: **"Directiva Equipo Local → Configuración del equipo → Plantillas administrativas → Componentes de Windows → Shell remoto de Windows".** 
140.	Seleccione la opción "Permitir acceso a Shell remoto". A continuación, pulse botón derecho y seleccione la opción del menú contextual "Editar". 
141.	A continuación, marque la opción "Habilitada" y pulse "Aceptar". 
142.	Para finalizar cierre el "Editor de directivas de grupo local".

ANEXO A.3.4. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA MEDIA DEL ENS PARA SERVIDORES IIS 10 SOBRE MICROSOFT WINDOWS SERVER 2016 EN ENTORNO INDEPENDIENTE

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar la sección de la guía "ANEXO A.3.3 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 INDEPENDIENTES SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS".

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores IIS 10 sobre Microsoft Windows Server 2016 independiente con implementación de seguridad de categoría media del ENS.

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

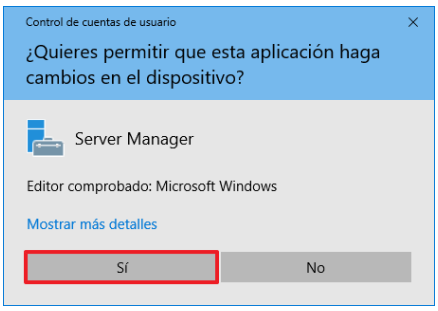
Para realizar las comprobaciones pertinentes en los servidores independientes se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor. Las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

a) Administrador del Servidor

b) Consola de servicios (services.msc)

c) Editor de registro (regedit.exe)

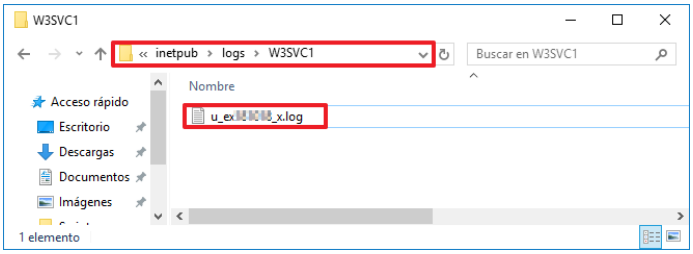
d) Explorador de Archivos (explorer.exe)

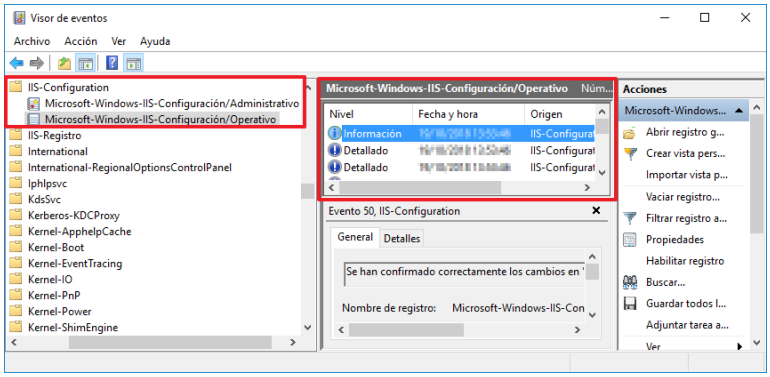
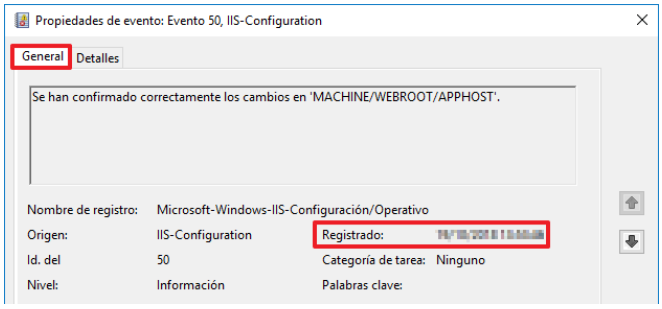
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el servidor a comprobar.		En uno de los servidores independiente, inicie sesión con una cuenta que tenga privilegios de administración. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Pulse "Sí" en la ventana de "Control de cuentas de usuario". 

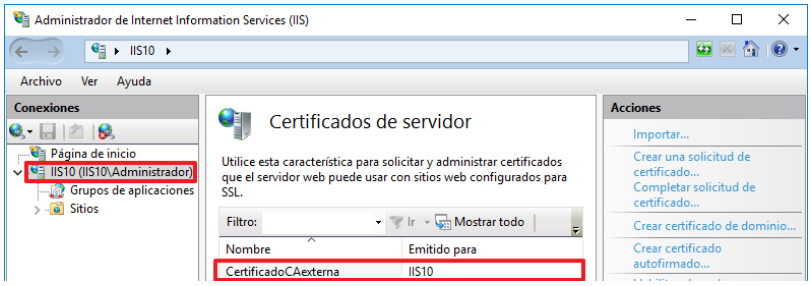
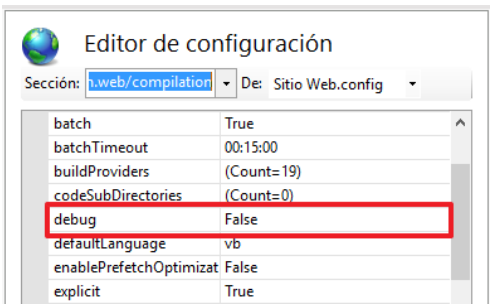
Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que los servicios del sistema están correctamente configurados		Usando la consola de servicios (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → services.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" para continuar. Verifique que el tipo de inicio de los servicios que aparecen en el sistema y en la siguiente tabla coinciden: **Nota:** Dependiendo de las características de IIS 10 instaladas en el equipo es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales.

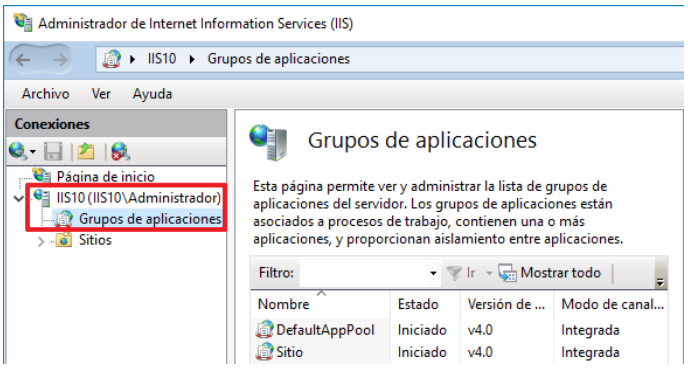
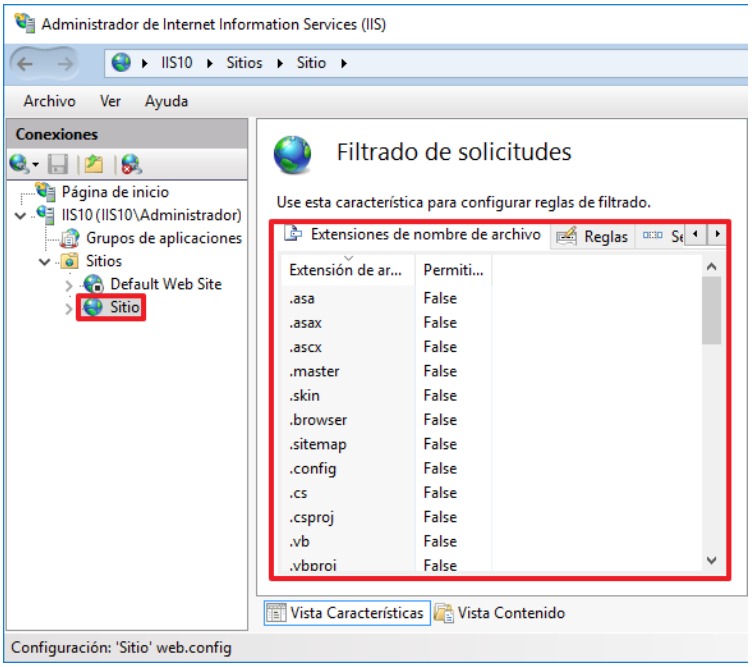
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio auxiliar de host para aplicaciones	AppHostSvc	Automático		
ASP.NET State Service	Aspnet_state	Automático		
Aplicación del sistema COM+	COMSysApp	Manual		
Servicio de administración IIS	IISADMIN	Automático		
Servicio de registro de W3C	w3logsvc	Automático		
Servicio de publicación World Wide Web	w3svc	Automático		
Servicio WAS	WAS	Automático		
Servicio de Administración Web	WMSVC	Manual		

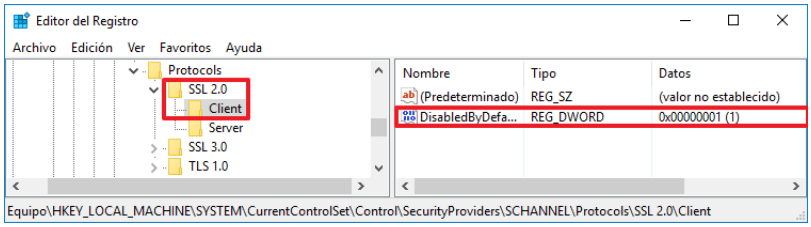
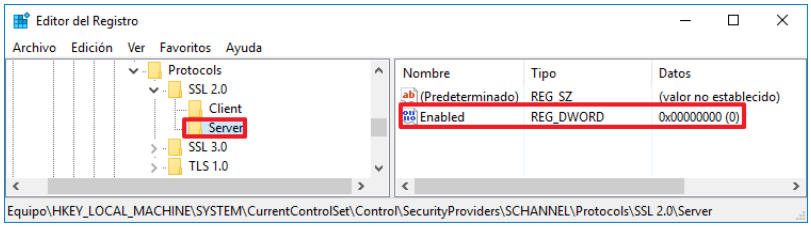
3. Verifique que se han asignado los permisos correctos en el sistema de archivos		Utilizando el Explorador de Windows: **"Windows+R → Explorer"** En caso de no saber dónde apunta cada una de las rutas abreviadas que se especifica, ejecute Explorer <<ruta>> donde <<ruta>> se sustituirá por la ruta abreviada. **Nota:** Para verificar los permisos de cada fichero o carpeta deberá abrir las propiedades del objeto, marcándolo con el botón derecho y eligiendo la opción "Propiedades" del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá situarse en la pestaña "Seguridad". En la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios. Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados.

Comprobación	OK/NOK	Cómo hacerlo			
Archivo			**Usuario**	**Permiso**	**OK/NOK**
%SystemRoot%\inetsrv\MetaBack			Administrador	Control total	
			System	Control total	
%SystemRoot%\LogFiles			Administrador	Control total	
			System	Control total	
			Creator Owner	Control total	
4. Compruebe que el registro de acceso de IIS está operativo.		En la configuración que ha realizado ha habilitado el registro de acceso al servidor, por lo que debe asegurarse que está registrando la actividad. Para ello verifique que el directorio **C:\inetpub\logs\W3SVC1** contiene ficheros con el formato **u_ex*fecha*.log**. Abriendo el último deberá ver que registra los accesos correctamente.  **Nota:** Tenga en cuenta que no se crea ningún registro hasta que no se realiza alguna actividad.			

Comprobación	OK/NOK	Cómo hacerlo
5. Verifique que los registros de Windows están habilitados		Los registros de aplicaciones y servicios integrados con el sistema operativo deben estar habilitados y almacenando información. Abra el Visor de eventos y busque: "**Menú inicio → Herramientas administrativas → Visor de eventos → Registros de aplicaciones y servicios → Microsoft → Windows → IIS-Configuration**".  Situándose sobre cada uno de ellos, abra el menú contextual, con el botón derecho del ratón, y compruebe que aparece la opción "Deshabilitar registro", lo cual indica que está habilitado.
6. Verifique que los registros son actuales.		Los dos registros deben contener eventos, abra ambos y compruebe que las últimas fechas de registro son recientes. 

Comprobación	OK/NOK	Cómo hacerlo
7. Comprobación certificado sitio web HTTPS		Dentro de la consola del "Administrador de Internet Information Services (IIS)" accedemos a "Certificados de servidor".  **Nota:** No olvide estar posicionado sobre el nombre del servidor y no sobre un determinado sitio o carpeta virtual, ya que todas las comprobaciones que está haciendo desde la consola de administración de IIS están siendo sobre el servidor. Se recomienda el uso de certificados EV en la categoría media del ENS.
8. Comprobación de la depuración de sistemas en producción.		Compruebe que la depuración en sistemas de producción esta deshabilitada. Para ello chequee: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS) → [nombre_del_servidor] → Sitios → Editor de configuración → Sección: System.web →Compilation → Debug →False"**. 

Comprobación	OK/NOK	Cómo hacerlo
9. Comprobación de las identidades del grupo de aplicaciones.		Compruebe que en las identidades del grupo de aplicaciones no hay identidades de servicio integradas. Para ello chequee: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS) → [nombre_del_servidor] → Grupo de aplicaciones"**. 
10. Comprobación del filtrado de solicitudes.		Compruebe que está habilitado el filtrado de solicitudes. Para ello chequee: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS) → [nombre_del_servidor] → Filtrado de solicitudes"**.  **Nota:** Dependiendo de la configuración en el filtrado de las solicitudes que se han configurado en el IIS 10 es posible que no aparezcan todos los filtros aquí relacionados o que aparezcan otros adicionales.

Comprobación	OK/NOK	Cómo hacerlo
11. Compruebe que se encuentran deshabilitados los algoritmos SSL2, SSL3 y TLS 1.0.		Compruebe que el uso de los algoritmos SSL2, SSL3 y TLS 1.0 estén deshabilitados. Utilizando el Explorador de Windows: **"Windows+R → Regedit.exe"** Y a continuación diríjase a: "**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols"** Compruebe que existen las carpetas con los 3 algoritmos y que contienen las carpetas "Client" y "Server". Compruebe el contenido de la carpeta "Client", tal y como se muestra a continuación.  Compruebe el contenido de la carpeta "Server", tal y como se muestra a continuación. 

ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.4.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 MIEMBROS DE DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS/DIFUSIÓN LIMITADA

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tenga que securizar IIS 10 sobre Microsoft Windows Server 2016 con una categorización de seguridad alta según los criterios del Esquema Nacional de Seguridad. Este anexo será de igual aplicación cuando el sistema sobre el que se esté aplicando seguridad cumpla con los requisitos para una red clasificada con grado de clasificación Difusión Limitada. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para los servicios e información manejada por la organización correspondieran, al menos, a la categoría alta para alguno de ellos, deberá realizar las implementaciones según se referencian en el presente anexo.

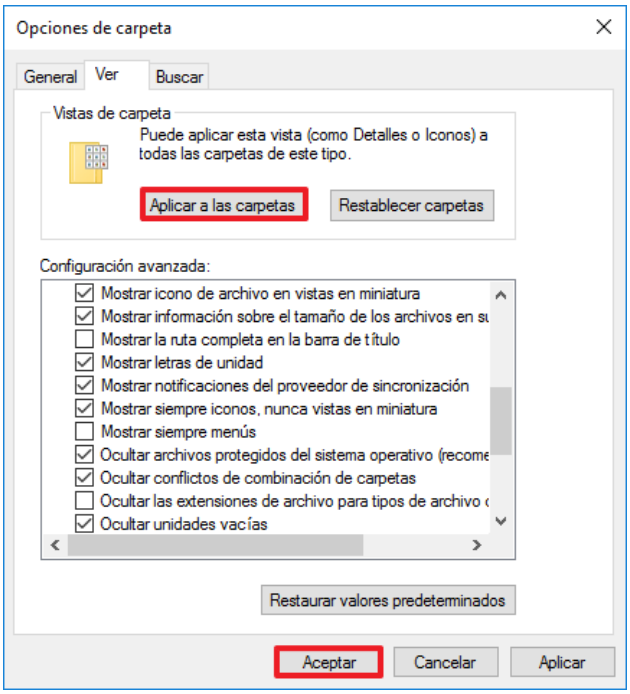
Este anexo será de igual aplicación cuando el sistema sobre el que se esté aplicando seguridad necesite cumplir los requisitos para una red clasificada con grado de clasificación Difusión Limitada.

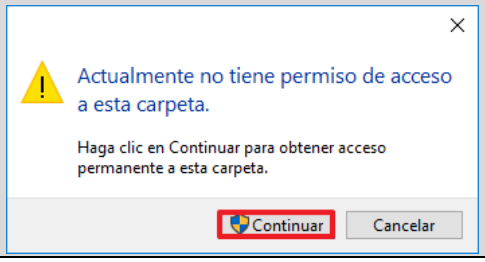
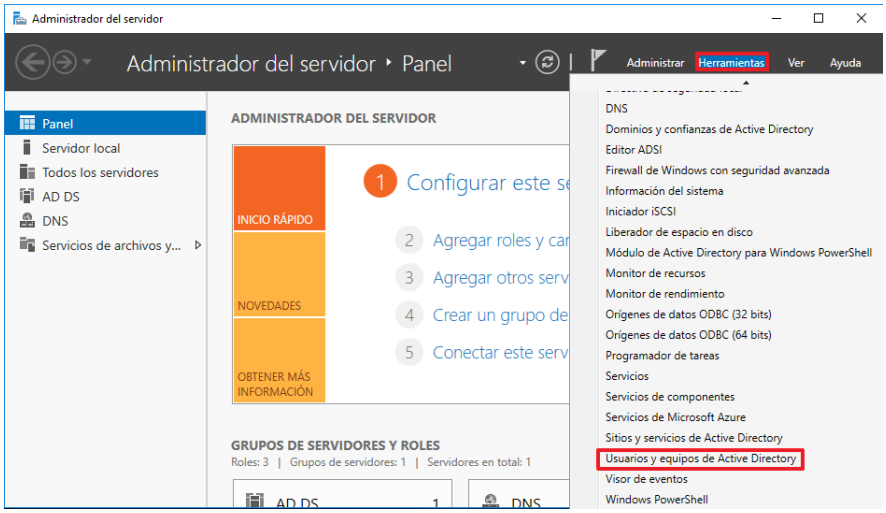
Nota: Tenga en cuenta que en el caso de una red clasificada con grado de clasificación Difusión Limitada se hará usó de la aplicación de seguridad descrita en este anexo, pero deberá atender adicionalmente a los requisitos establecidos por la normativa de aplicación sobre sistemas clasificados para dicho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

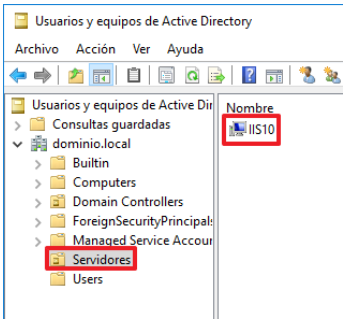
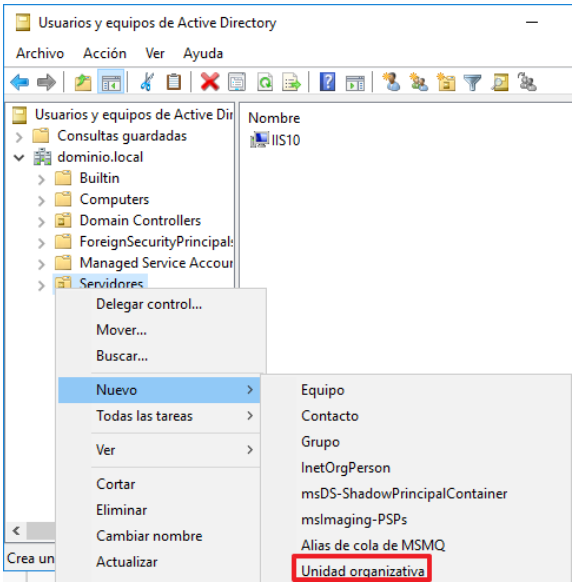
Debe tener en consideración que, antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad para comprobar su correcta funcionalidad.

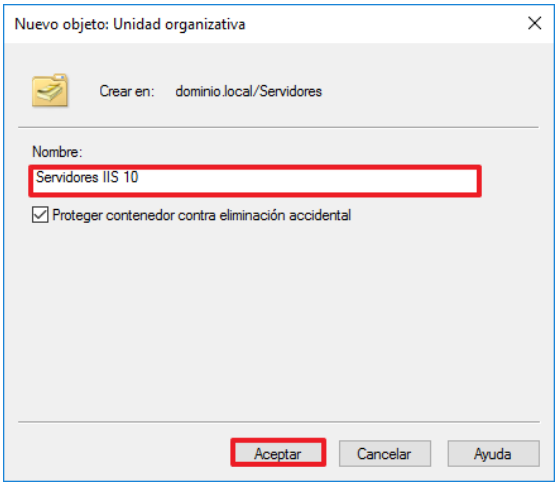
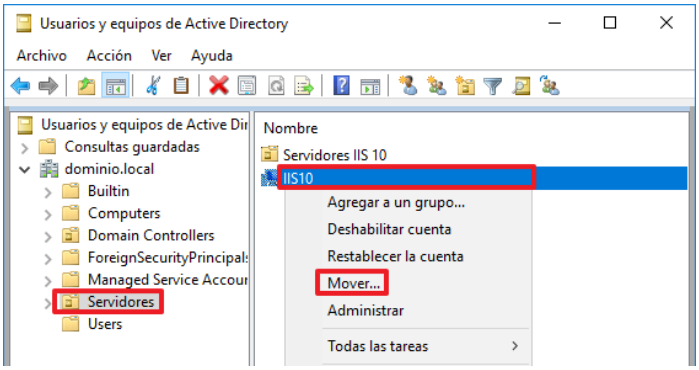
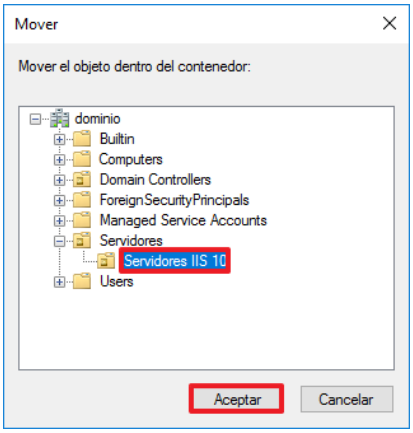
1. PREPARACIÓN DEL DOMINIO

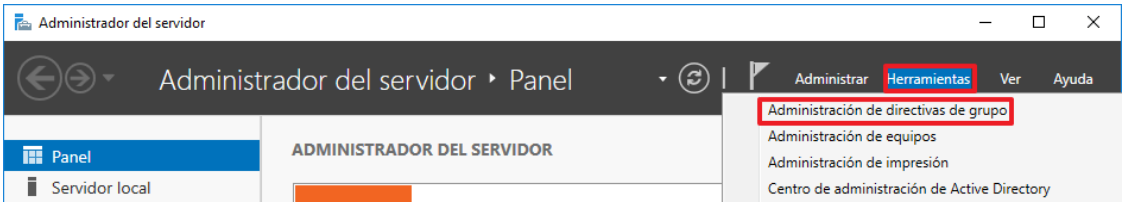
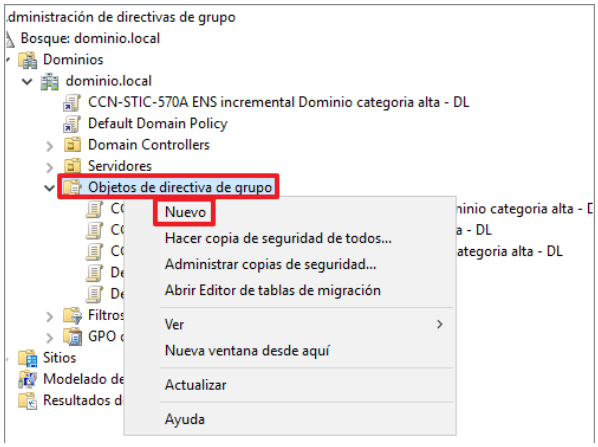
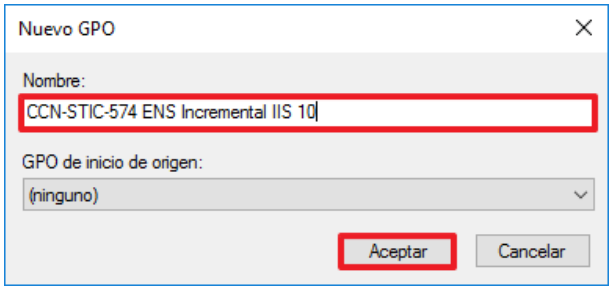
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.

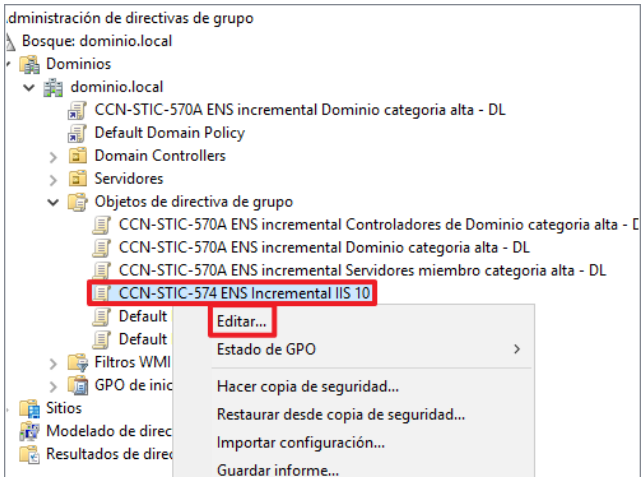
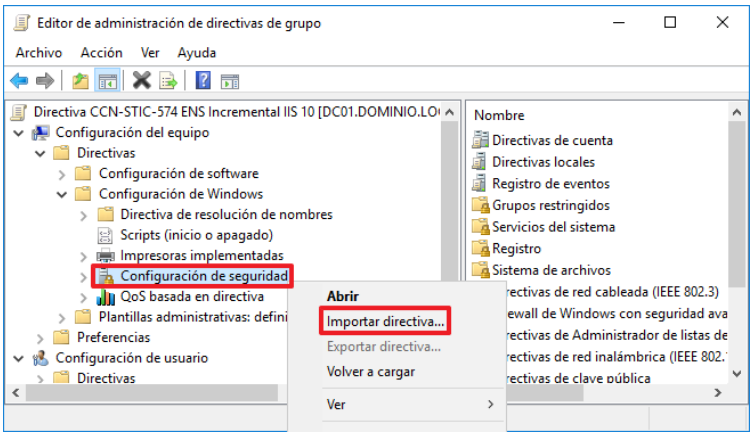
Paso	Descripción
2.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
3.	Copie los scripts y plantillas de seguridad asociadas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

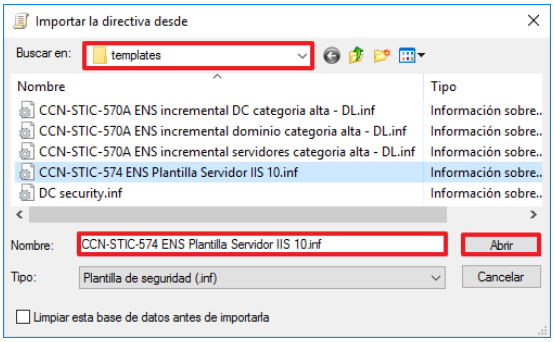
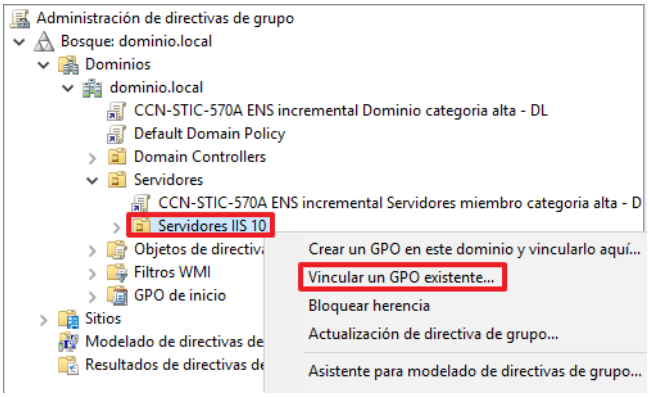
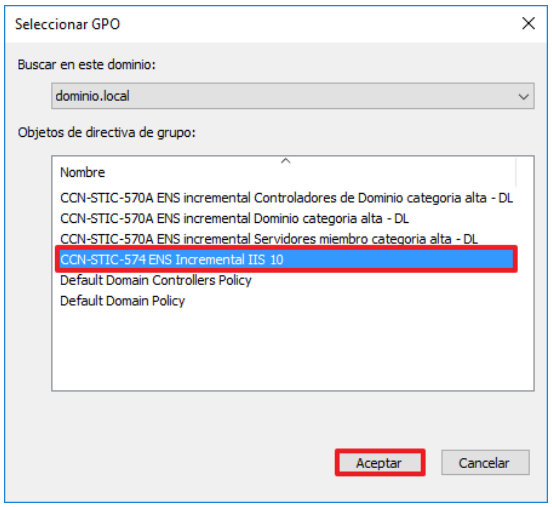
Paso	Descripción
5.	A continuación, copie el fichero “CCN-STIC-574 ENS Plantilla Servidor IIS 10.inf” al directorio “%SYSTEMROOT%\security\Templates” del controlador de dominio. **Nota:** Según la configuración de seguridad de UAC, el sistema podría solicitar la elevación de privilegios por cada uno de ellos, en este caso, pulse “Continuar” en las 3 ocasiones que el sistema se lo solicita o marque la opción “Hacer esto para todos los elementos actuales” para pulsar “Continuar” en una sola ocasión. 
6.	Inicie la herramienta de usuarios y equipos del Directorio Activo. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione **“Herramientas → Usuarios y equipos de Active Directory”** 

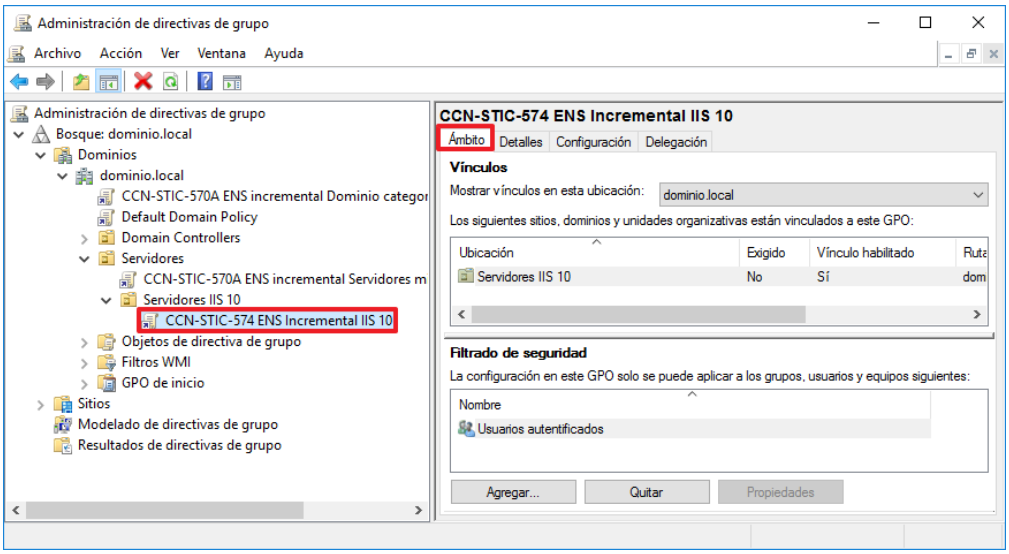
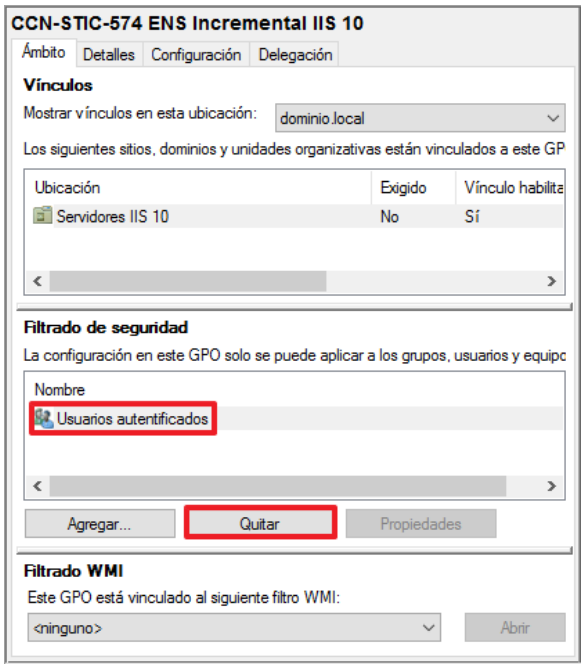
Paso	Descripción
7.	Despliegue el dominio y vaya a la unidad organizativa “Servidores”. “**Menú inicio → Herramientas administrativas →Usuarios y equipos de Active Directory → [nombre del dominio] → Servidores**”.  **Nota:** Si usted no desea crear unidades organizativas en su organización deberá adaptar estos pasos para alojar los servidores IIS 10 y vincular la GPO que se creará posteriormente a los servidores IIS 10 de su organización.
8.	Solicite la creación de una nueva unidad organizativa utilizando el menú contextual, pulse botón derecho sobre la unidad organizativa “Servidores” y despliegue **“Nuevo → Unidad organizativa”**. 

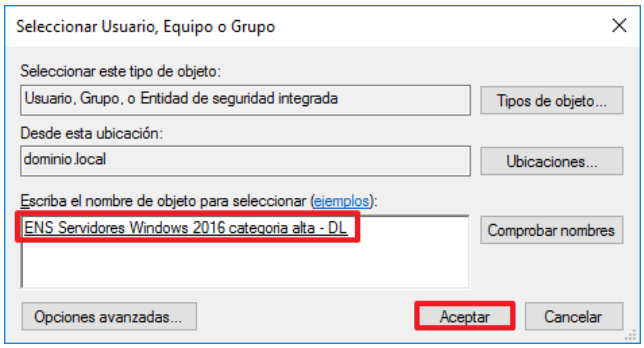
Paso	Descripción
9.	En la consola, cree una unidad organizativa denominada “Servidores IIS 10” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen. 
10.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores IIS 10 a la unidad organizativa “Servidores IIS 10”. Para ello, deberá hacer clic botón derecho sobre “mover” en el servidor que desee ubicar en la nueva unidad organizativa. 
11.	A continuación, seleccionamos la unidad organizativa “Servidores IIS 10”. 

Paso	Descripción
12.	Cierre la herramienta de “Usuarios y equipos de Directorio Activo”
13.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”** 
14.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”.
15.	Pulse con el botón derecho, sobre dicha y carpeta y seleccione la opción “Nuevo”. 
16.	Introduzca como nombre “CCN-STIC-574 ENS Incremental IIS 10” y pulse el botón “Aceptar”. 

Paso	Descripción
17.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
18.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**
19.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva…”. 

Paso	Descripción
20.	Seleccione de la ruta “C:\Windows\security\templates” el fichero “CCN-STIC-574 Plantilla Servidor IIS 10” y pulse el botón “Abrir”. 
21.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
22.	A continuación, seleccione la unidad organizativa “Servidores IIS 10” y pulse botón derecho, “Vincular un GPO existente…”. 
23.	Seleccione el objeto de directiva de grupo con nombre, “CCN-STIC-574 ENS Incremental IIS 10” y pulse aceptar. 

Paso	Descripción
24.	Cierre la política de grupo.
25.	Seleccione la nueva política de grupo configurada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 
26.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
27.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación.
28.	Una vez quitado, pulse el botón “Agregar…”.

Paso	Descripción
29.	Introduzca como nombre “ENS servidores Windows 2016 categoria alta - DL”. Este grupo corresponde con el generado en la aplicación de la guía CCN-STIC-570A. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.

2. CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

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

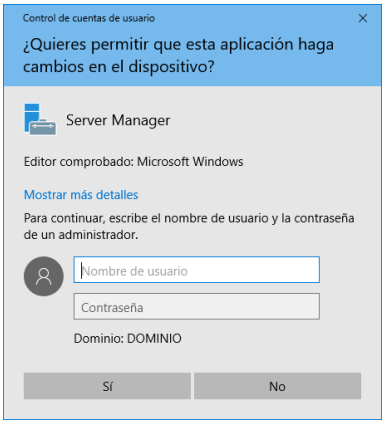
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

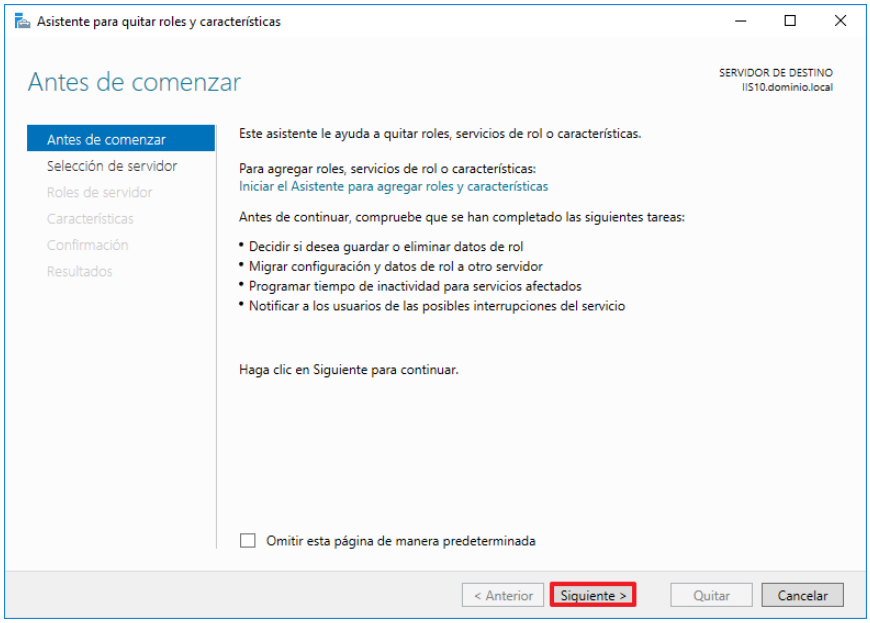
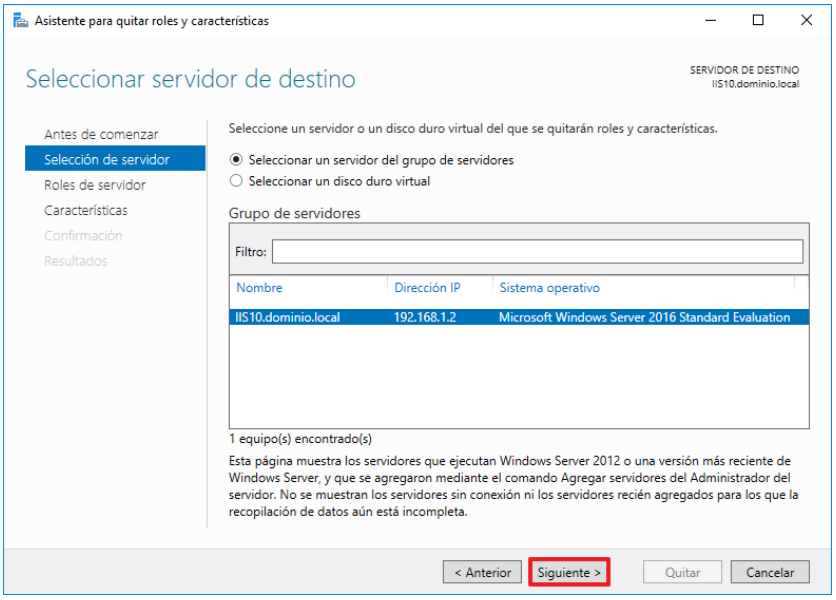
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

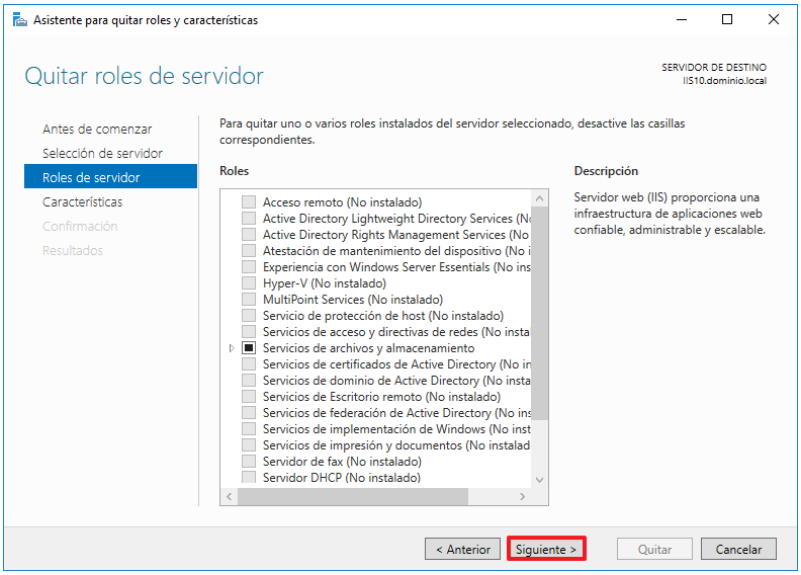
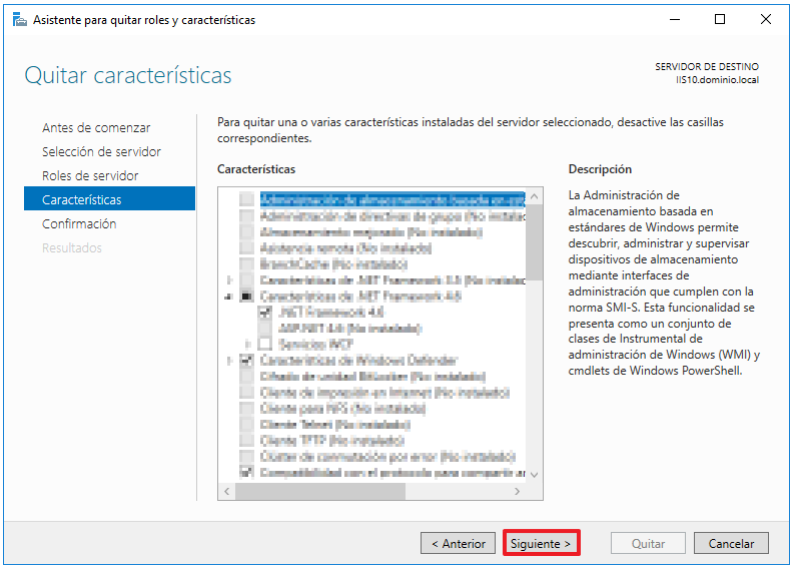
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

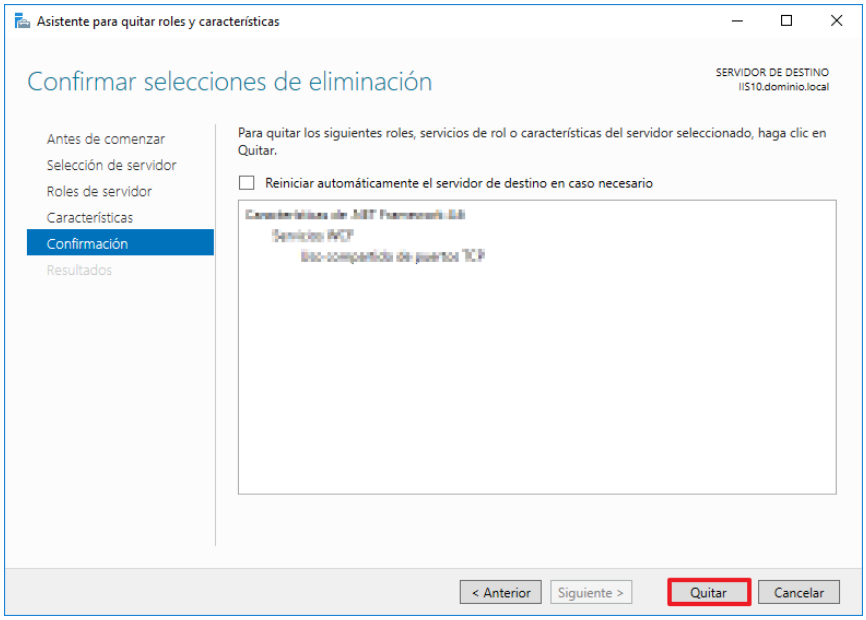
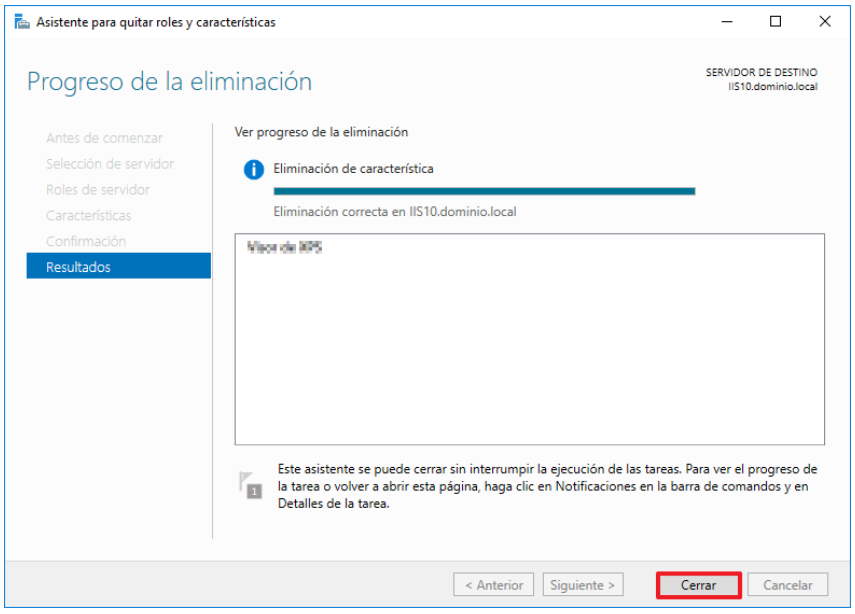
Es recomendable que el sitio web este alojado en otra ubicación de disco diferente a la del sistema operativo y que esta solo se utilice para el alojamiento de sitios web, evitando con ello exponer más información de la estrictamente necesaria.

Para realizar el siguiente paso a paso deberá realizar previamente el paso “3.1 PREPARACIÓN DEL DIRECTORIO ACTIVO” y una vez finalizado deberá realizar el paso “3.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

Paso	Descripción
30.	A continuación, deberá iniciar sesión en el servidor miembro donde está instalado el rol de IIS 10.
31.	Pulse sobre el administrador del servidor. 
32.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 
33.	A continuación, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione **“Administrar → Quitar roles y funciones”**. 

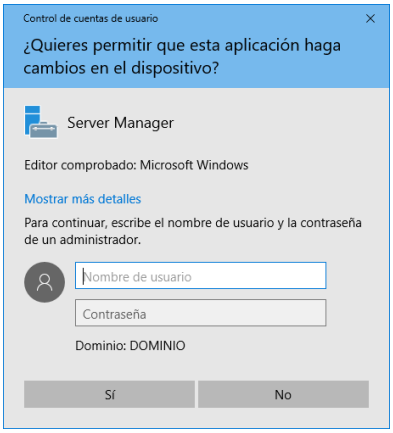
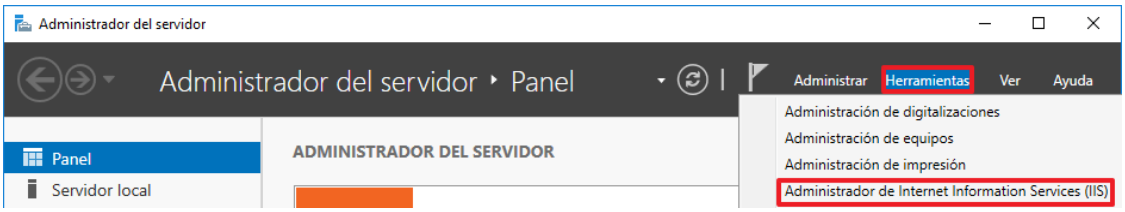
Paso	Descripción
34.	Comenzará el asistente para quitar roles y características, pulse sobre el botón “Siguiente >”. 
35.	Seleccione el servidor donde desea quitar las características del IIS 10 y pulse siguiente. 

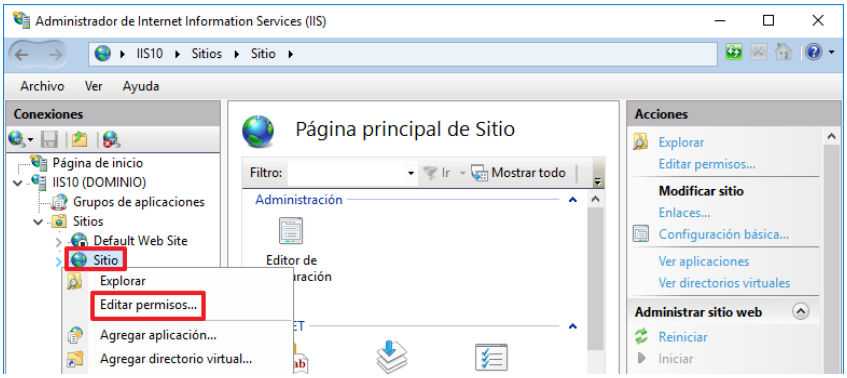
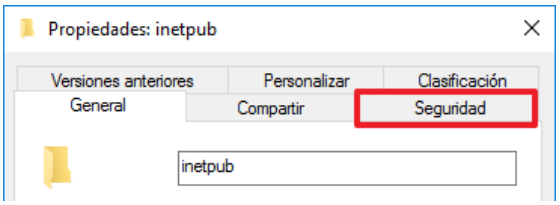
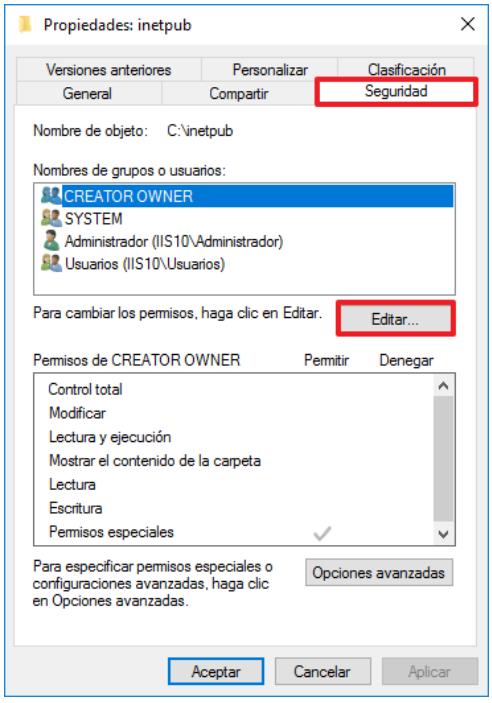
Paso	Descripción
36.	En la siguiente ventana podrá quitar roles del servidor, en este caso pulse siguiente para acceder a las características de los roles instalados. 
37.	A continuación, seleccione las características que desea quitar. 

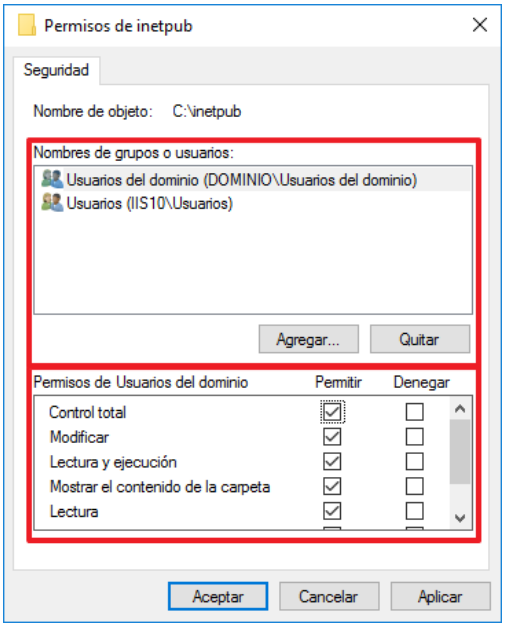
Paso	Descripción
38.	La siguiente pantalla mostrara las características a modos resumen que desea quitar, confirme que las características seleccionadas son las correctas y pulse “Quitar”. 
39.	Una vez finalizada la desinstalación pulse “Cerrar”.  **Nota:** Debe tener en cuenta que la desinstalación de determinadas características puede requerir el reinicio del equipo.

2.2. GESTION DE PERMISOS RECURSOS WEB

En este apartado se tendrá en consideración la gestión y administración del acceso a los recursos web según el marco operacional de categoría alta establecido por el ENS, para con ello limitar y controlar el acceso a directorios con información sensible de ser sustraída.

Paso	Descripción
40.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
41.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 
42.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione: **“Herramientas → Administrador de Internet Information Services (IIS)”** 

Paso	Descripción
43.	Pulse botón derecho sobre el sitio al cual quiere asignar o quitar permisos. 
44.	Diríjase hasta la pestaña seguridad. 
45.	A continuación, pulse el botón “Editar”. 

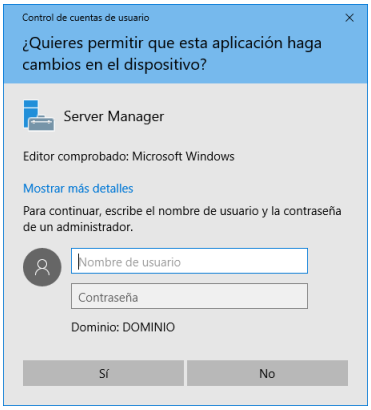
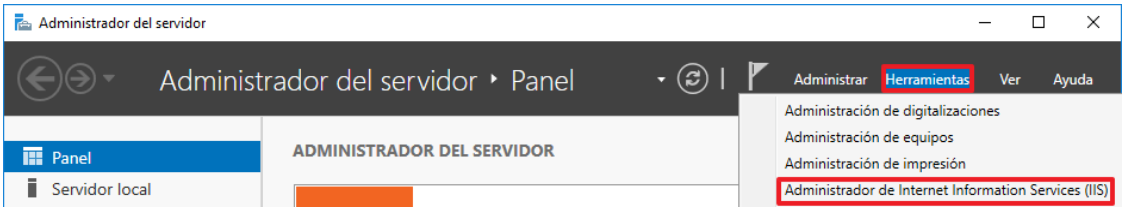
Paso	Descripción
46.	A continuación, seleccione los permisos del que desea establecer para ese sitio web.  **Nota:** Es recomendable dar permiso solo a los usuarios o grupos que deban tener acceso al sitio web evitando que el usuario administrador tenga permiso para prevenir posibles vulnerabilidades.

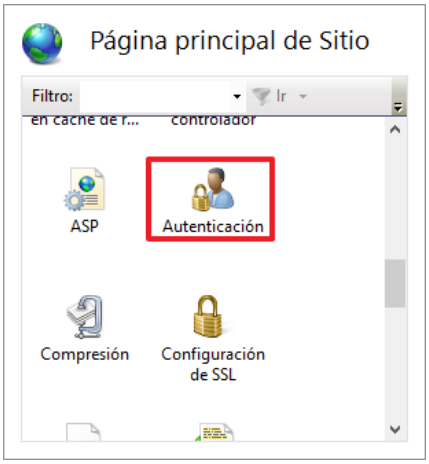
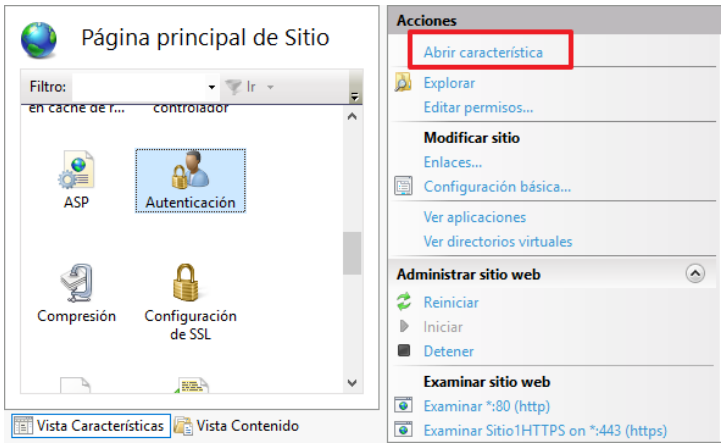
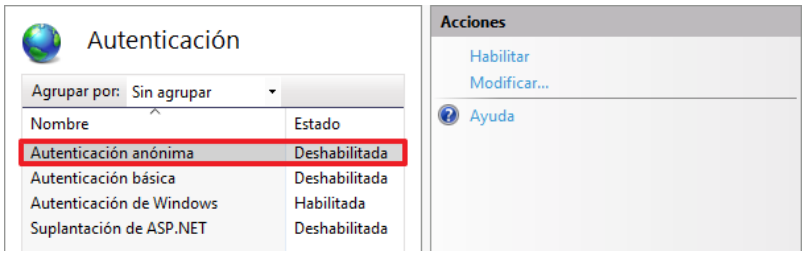
2.3. AUTENTICACIÓN SITIO WEB

Los métodos de autenticación permiten limitar el acceso al sitio web a una lista determinada de usuarios (el método habilitado por defecto de los servicios web de IIS es la autenticación anónima), en la categoría alta de categorización del ENS se recomienda habilitar los mecanismos de autenticación basados en el uso de certificados biométricos o certificados emitidos por terceros.

El siguiente paso a paso indica como habilitar un certificado de terceros.

Paso	Descripción
47.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 

Paso	Descripción
48.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 
49.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione: **“Herramientas → Administrador de Internet Information Services (IIS)”**. 
50.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo de “Conexiones” y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.

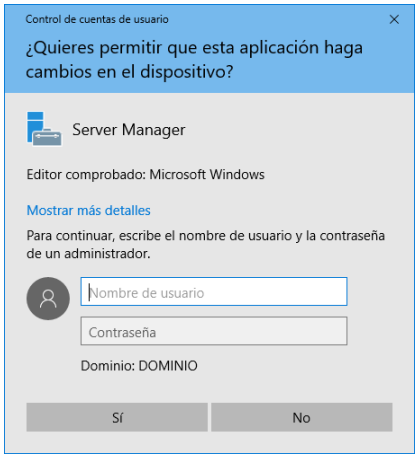
Paso	Descripción
51.	Seleccione en la página principal del sitio web el icono de “Autenticación”. 
52.	Pulse sobre “Abrir característica” situado en el panel derecho en el menú “Acciones”. 
53.	A continuación, establezca según las características de su organización los métodos de autenticación disponibles. Para ello pulse sobre el método de autenticación que quiere configurar y en el panel derecho seleccione la acción que desea realizar.  **Nota:** Únicamente se usará la autenticación anónima para páginas webs generales en la que solo se muestre contenido y no sea necesaria la autenticación del usuario.

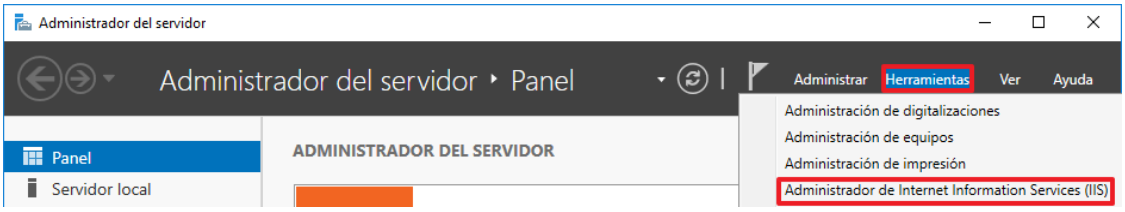
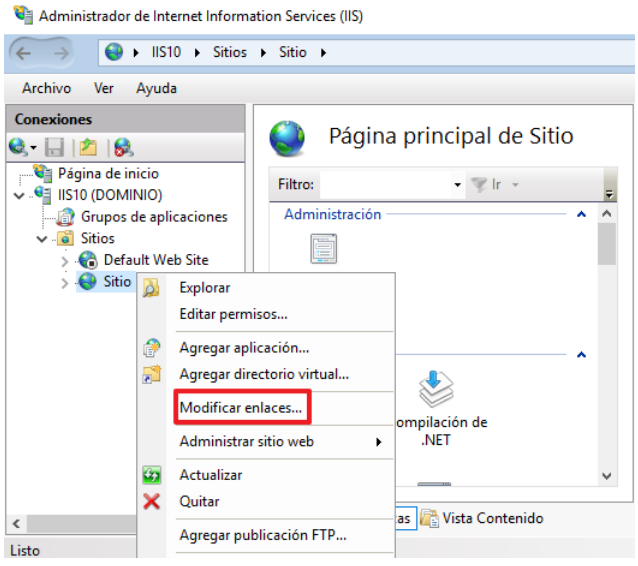
2.4. CERTIFICADOS

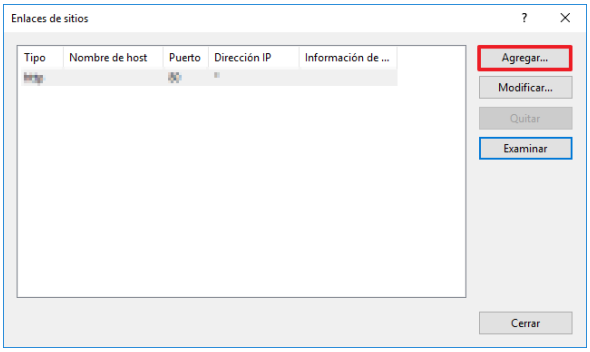
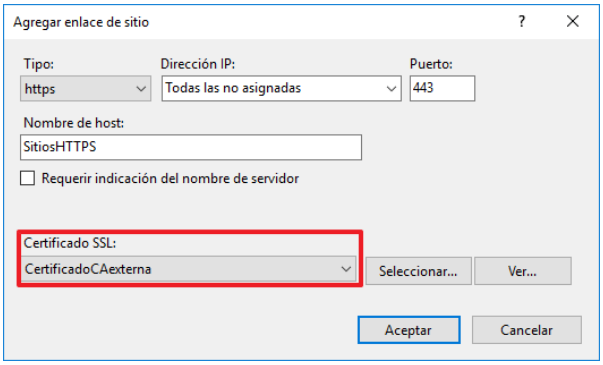
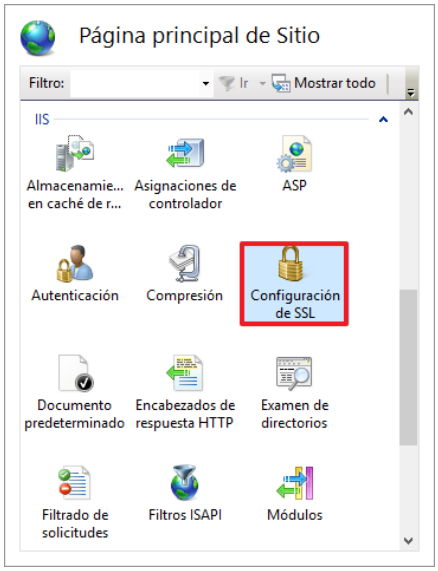
IIS 10 faculta el empleo de protocolos seguros para las comunicaciones y los procesos de autenticación usando HTTPS que utiliza un cifrado basado en SSL/TLS para crear un canal cifrado para el tráfico de información sensible. Para lugares públicos es un requisito indispensable en la categoría media y alta de seguridad del ENS el uso de certificados emitidos por entidades certificadoras de terceros, para el caso de sitios internos se recomienda el uso de certificados emitidos por una entidad certificadora interna, está totalmente desaconsejado el uso de certificados autofirmados.

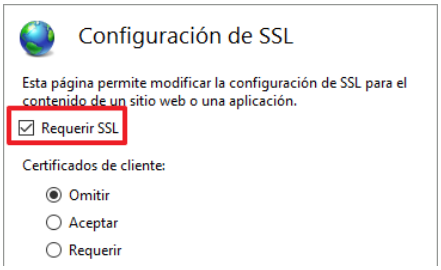
Para la categoría más alta de seguridad del ENS es aconsejable el uso de certificados biométricos los cuales se basan en la medición de una característica física inmutable de una persona para identificar a esa persona de forma única. Las huellas digitales son una de las características biométricas más comunes.

Nota: Si desea obtener más información sobre la autenticación mediante los certificados biométricos puede consultar la siguiente página web:
https://docs.microsoft.com/en-us/windows/desktop/SecBioMet/biometric-service-api-portal

Paso	Descripción
54.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
55.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 

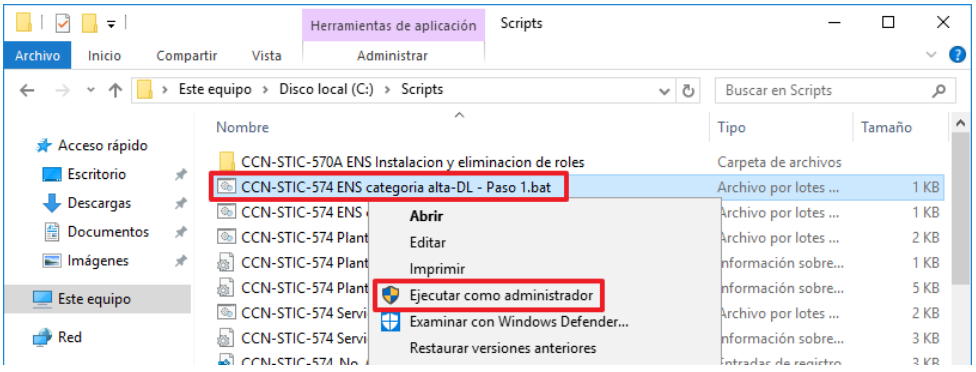
Paso	Descripción
56.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione: **“Herramientas → Administrador de Internet Information Services (IIS)”** 
57.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo de “Conexiones” y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.
58.	Pulse con el botón derecho sobre el sitio web que quiere modificar y seleccione la opción “Modificar enlaces…”. 

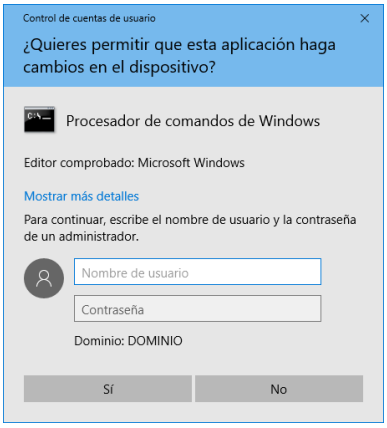
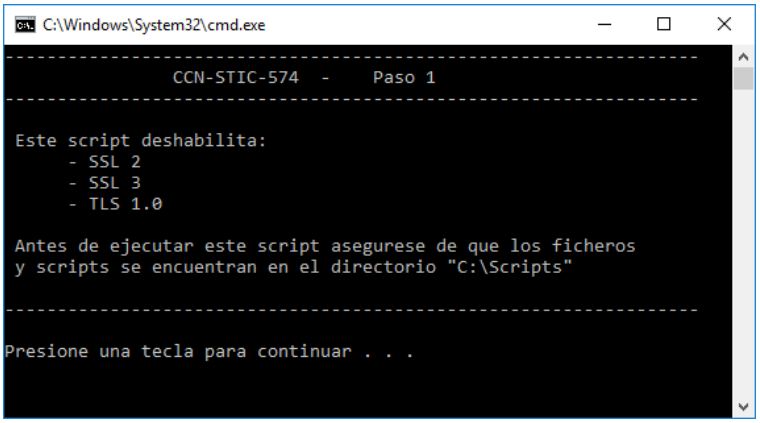
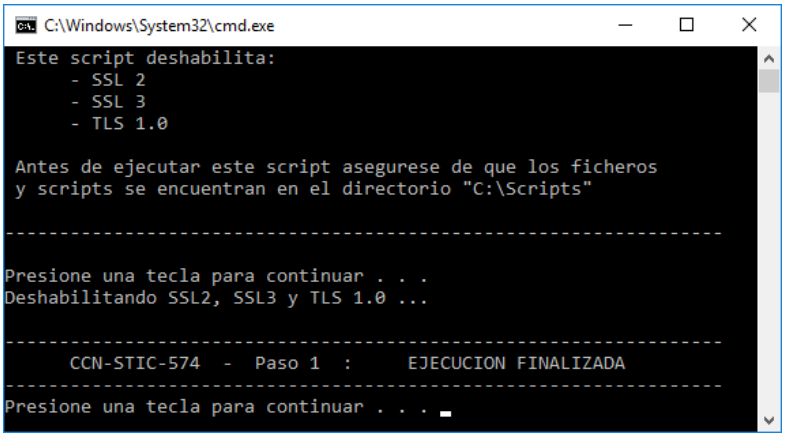
Paso	Descripción
59.	Pulse sobre el botón “Agregar…”. 
60.	Seleccione Tipo: “Https” y a continuación seleccione el Certificado SSL de una entidad externa y pulse “Aceptar”. 
61.	A continuación, deberá configurar el sitio web para que los usuarios requieran un certificado propio, para ello pulse sobre en el sitio web que desea configurar, y seleccione “Configuración de SSL”. 

Paso	Descripción
62.	Seleccione la opción de “Requerir SSL” y pulse sobre “Aplicar” para que el sistema guarde los cambios realizados. 
63.	En caso de que usted no cuente con un certificado emitido por una entidad certificadora autorizada debe solicitarlo para cumplir con la categoría alta de seguridad del ENS.

2.5. PROTOCOLOS DE TRANSMISIÓN

Con la aplicación del ENS para la categoría alta sobre IIS 10 es imprescindible eliminar el uso de los algoritmos SSL2, SSL3 y TLS1.0, evitando con ello sufrir posibles ataques.

Paso	Descripción
64.	Inicie sesión en el servidor miembro donde tiene instalado el rol de IIS 10.
65.	Si no lo ha realizado anteriormente, cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
66.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.
67.	A continuación, debe ejecutar el *script* 1 para deshabilitar los protocolos anteriormente indicados, es necesario realizar esta acción con elevación de privilegios, debe hacer clic con el botón derecho, sobre el fichero denominado “CCN-STIC-574 ENS categoria alta-DL – Paso 1.bat” situado en “C:\Scripts” y haga clic en “Ejecutar como administrador”. 

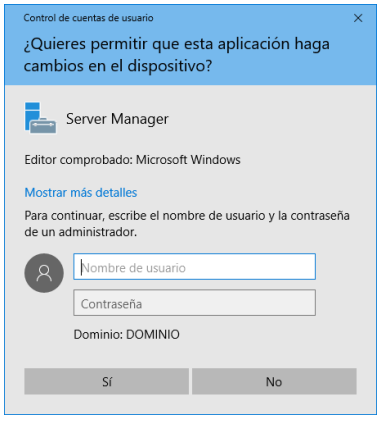
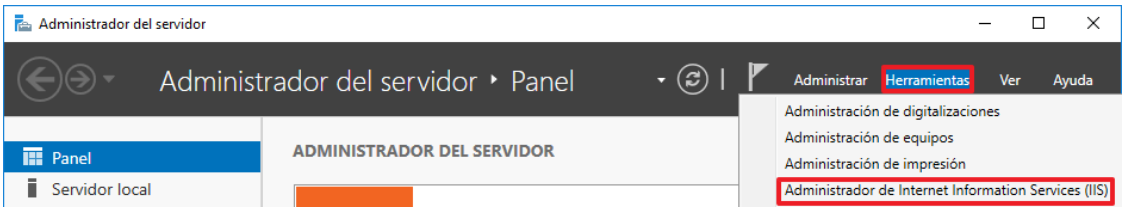
Paso	Descripción
68.	El control de cuentas de usuario le solicitará permisos para ejecutar el programa.  **Nota:** En caso de solicitar elevación de privilegios debe introducir un usuario con permisos de administración.
69.	Aparecerá la siguiente ventana, pulse cualquier tecla para continuar. 
70.	Una vez finalizada la tarea pulse una tecla para cerrar la ventana. 

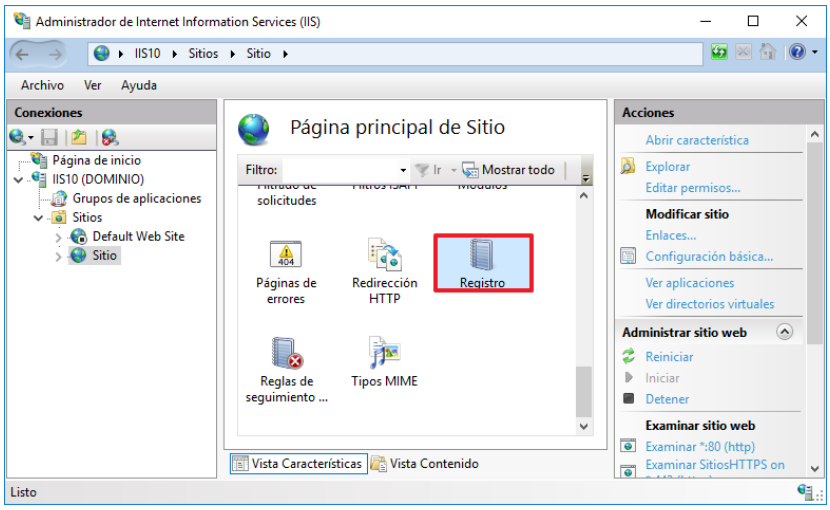
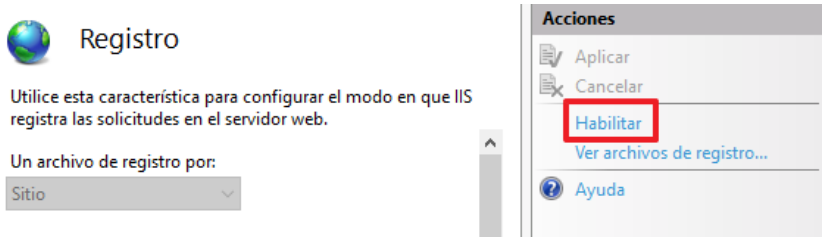
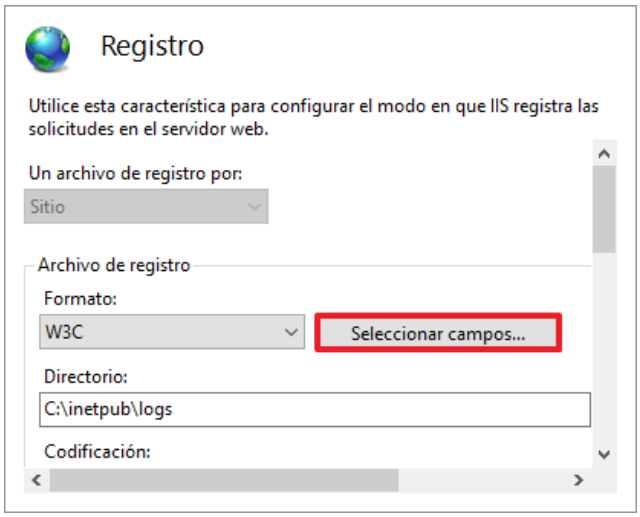
2.6. AUDITORÍA

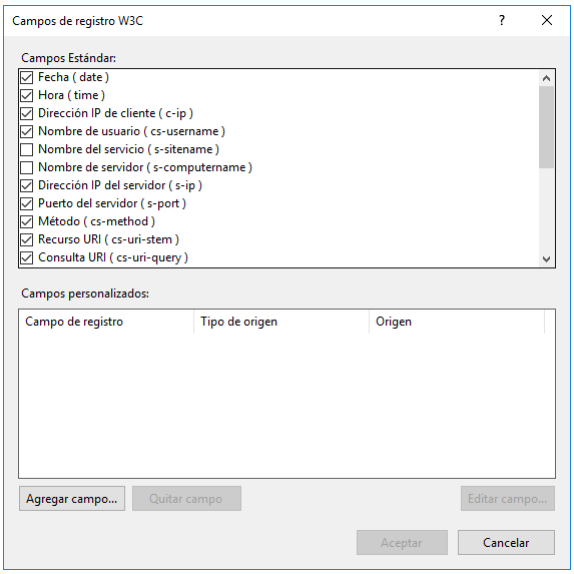
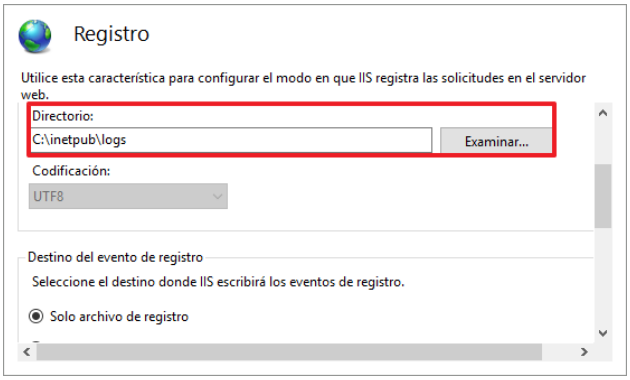
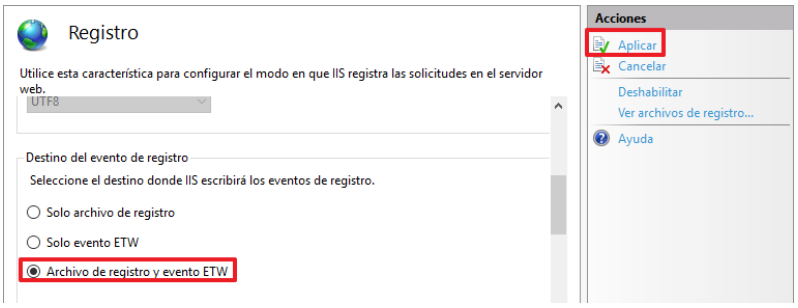
Con la aplicación del ENS para la categoría alta o Difusión Limitada sobre IIS 10 quedará registrado el uso del sistema para poder detectar y reaccionar a cualquier fallo accidental o deliberado, quedando registrado en el sistema quien realiza la actividad, cuando y sobre qué información con el fin de detectar anomalías o intentos frustrados de acceso a información no autorizada.

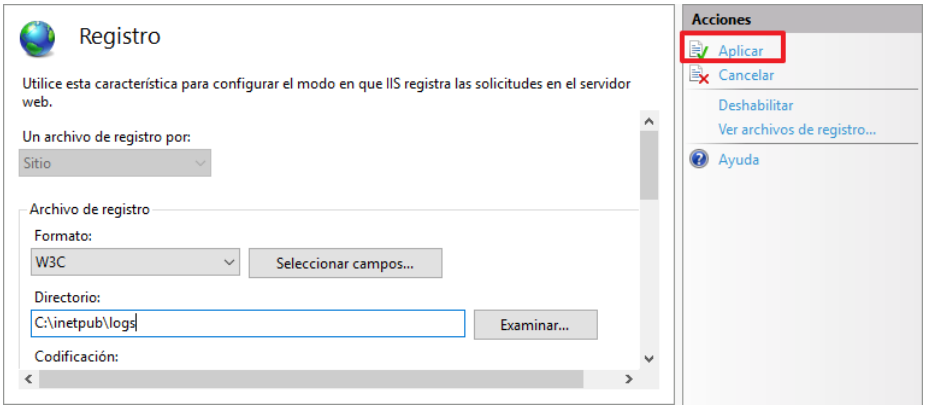
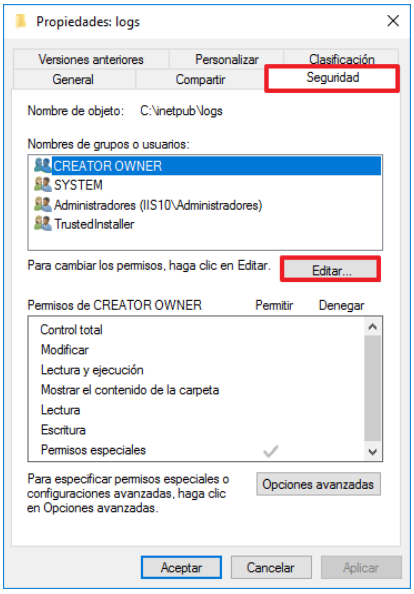
La ubicación de los registros debe ser diferente a la del sistema además de tener limitado el acceso únicamente a los usuarios autorizados.

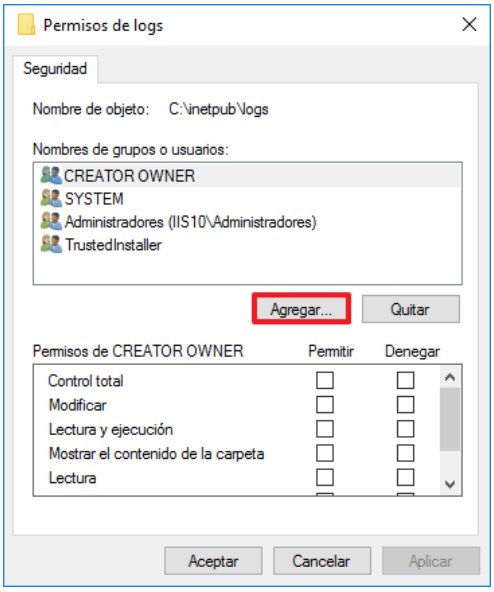
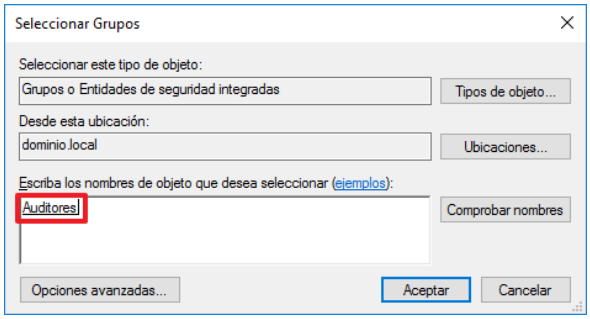
Es recomendable en la categoría alta del marco del ENS el uso de herramientas de consolidación de eventos con el fin de tener centralizada toda la información relevante obtenida de los registros en un único punto y en orden cronológico. Muchas herramientas de consolidación son capaces de elaborar alertas más elaboradas basándose en los eventos recibidos de las diversas fuentes de información.

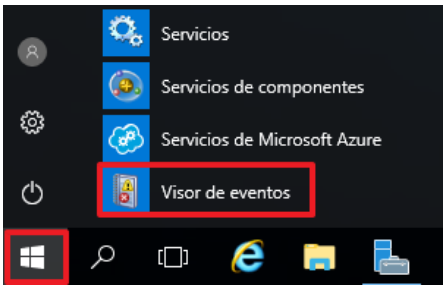
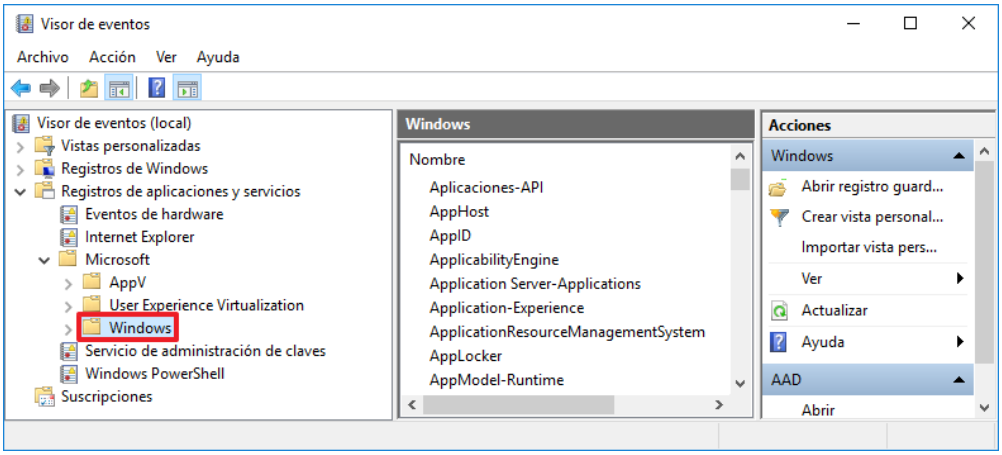
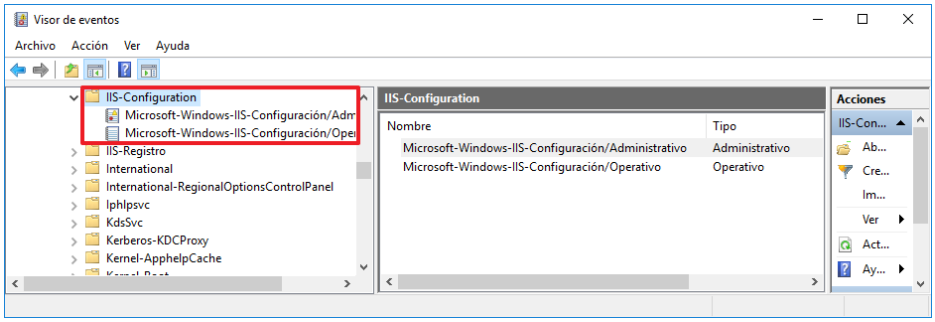
Paso	Descripción
71.	Inicie sesión en el servidor miembro donde tiene instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
72.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 
73.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”** 

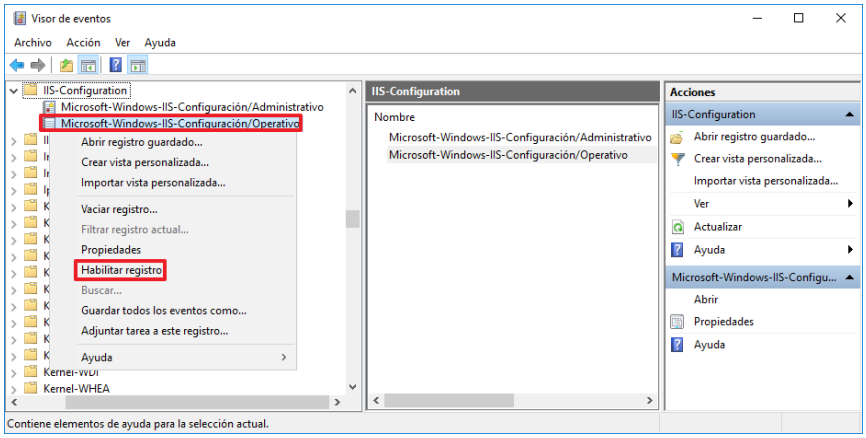
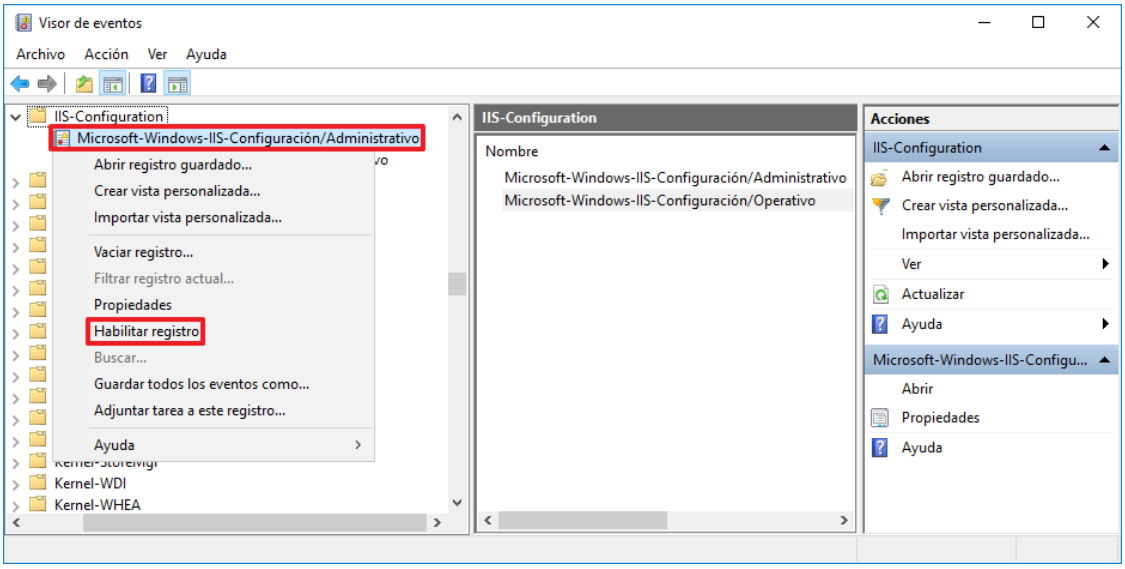
Paso	Descripción
74.	Diríjase al sitio web que desea administrar, a continuación, localice el icono “Registro”, y pulse la acción “Abrir característica” situado en la parte superior derecha de la pantalla para acceder a la configuración del registro. 
75.	Debe habilitar el registro de las solicitudes del servidor IIS 10 para ello, diríjase al menú “Acciones” situado en la parte superior derecha de la pantalla y pulse sobre “Habilitar”. 
76.	Seleccione los campos que desea registrar, para ello pulse sobre “Seleccionar campos…”. 

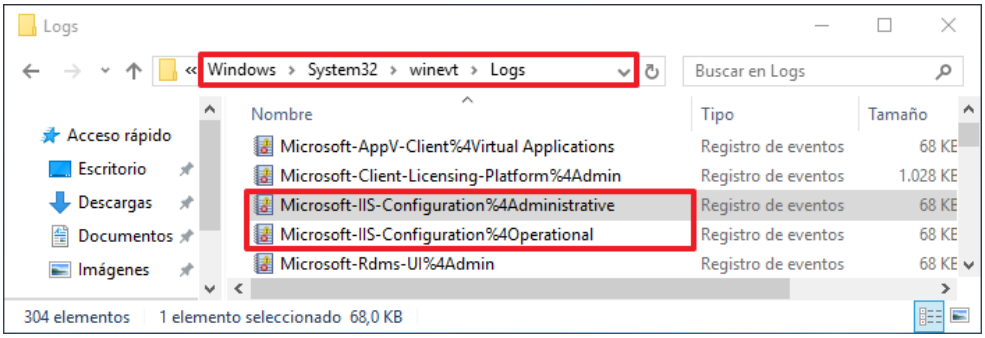
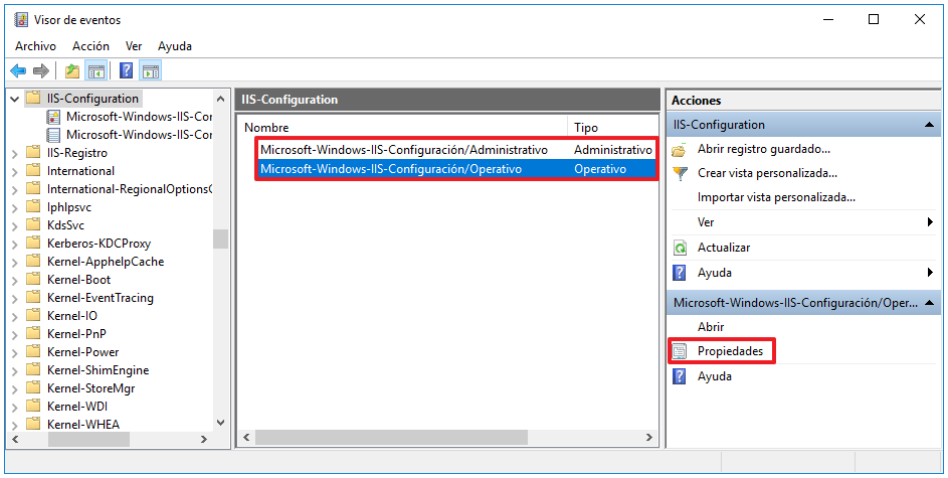
Paso	Descripción
77.	Compruebe qué campos se recogerán en el fichero de registro y asegúrese que coincide con sus necesidades. Los valores marcados por defecto suelen ser suficientes, pero no descarte marcar otros. 
78.	A continuación, seleccione el directorio donde se van a guardar los registros, por seguridad es recomendable realizarlo en una unidad diferente a la de la instalación del sistema operativo. 
79.	A continuación, deberá seleccionar el destino del evento, seleccione, “Archivo de registro y evento ETW”. 

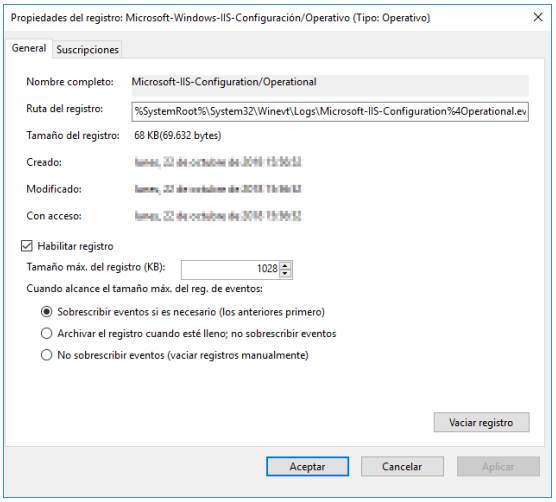
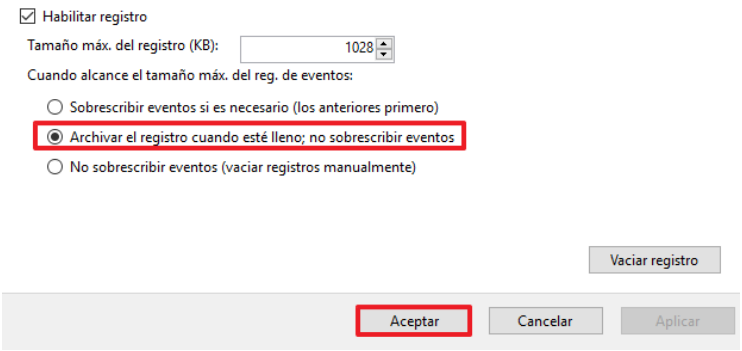
Paso	Descripción
80.	Una vez realizados los cambios deberá guardarlos, para ello pulse “Aplicar” situado en el menú “Acciones” en la parte superior izquierda de la pantalla. 
81.	A continuación, localice la carpeta **C:\INETPUB\logs**, y con el botón derecho seleccione “Propiedades”. **Nota:** Si no dispone de la carpeta “C:\INETPUB\logs” deberá crearla o adaptar los pasos a su organización.
82.	Sitúese en la pestaña “Seguridad”, donde observa que la carpeta tiene permisos aplicados directamente (los *tics* en la columna “Permitir” están en negro, no en aguadilla).  Presione “Editar” para modificar los permisos. Se detalla a continuación la actuación. **Nota:** Los permisos aplicados al usuario que ha tomado posesión de la carpeta son normales y puede ignorarlos o eliminarlos. Si el usuario no está autorizado a auditar ficheros de registro o se desea cambiar se debe hacer en la carpeta desde donde se heredan los permisos de ésta, C:\INETPUB\logs

Paso	Descripción
83.	Presione el botón “Agregar…”. 
84.	Escriba “Auditores” y acepte para que se añada.  **Nota:** Si no dispone del grupo Auditores deberá crearlo previamente para poder añadirlo.
85.	Los permisos que se adjudican por defecto, lectura, para los “Auditores” son los deseados por lo que puede continuar el proceso haciendo clic en el botón “Aceptar” en la ventana “Permisos de logs”, y de nuevo “Aceptar” en la ventana “Propiedades: logs”.
86.	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.

Paso	Descripción
87.	Debe abrir el Visor de eventos, ejecutándolo como administrador, como en ocasiones anteriores: "**Menú inicio→ Herramientas administrativas→ Visor de eventos**".  **Nota:** El sistema solicitará elevación de privilegios para completar la acción.
88.	Seleccione en el árbol **"Visor de eventos → Registro de aplicaciones y servicios → Microsoft → Windows"**. 
89.	Desplácese hacia abajo, podrá observar que Microsoft Windows Server 2016 dispone de dos grupos de registros para IIS, dentro del de configuración se encuentran: administrativo y operaciones. Es necesario activar ambos, según se le indica a continuación. 

Paso	Descripción
90.	Sitúese sobre el registro operativo, abra el menú contextual con el botón derecho del ratón y seleccione “Habilitar registro”.  **Nota:** Cualquier acción operativa sobre el servidor quedará recogida a partir de ahora.
91.	Haga lo mismo para el registro “Administrativo”. 

Paso	Descripción
92.	Los registros se habrán creado en el disco duro, en la partición del sistema operativo (habitualmente la C:) y en la ruta **%SystemRoot%\System32\winevt\Logs**, con los nombres: Microsoft IIS-Configuration%4Operational.evtx y Microsoft IIS-Configuration%4Administrative.evtx  **Nota:** La variable %SystemRoot% corresponde a C:\Windows\System32 en las configuraciones habituales de las guías.
93.	Los ficheros se crean con tamaño cero pero se empezarán a poblar automáticamente desde este momento: **IIS-Configuration** Nombre / Tipo / Número de eventos / Tamaño Microsoft-Windows-IIS-Configuración/Administrativo — Administrativo — 0 — 68 KB Microsoft-Windows-IIS-Configuración/Operativo — Operativo — 0 — 68 KB
94.	Para acceder a las propiedades de los ficheros, seleccione un fichero y pulse sobre la opción “Propiedades” del menú “Acciones”.  **Nota:** Tenga en cuenta que el registro administrativo se llenará, en condiciones normales, antes que el operacional.

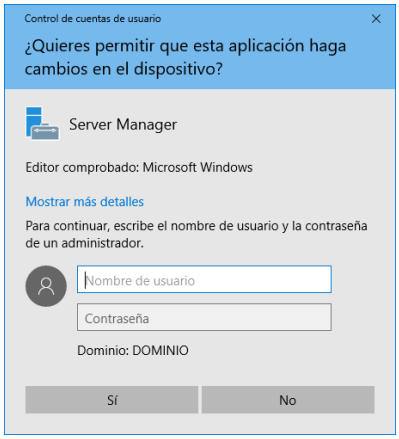
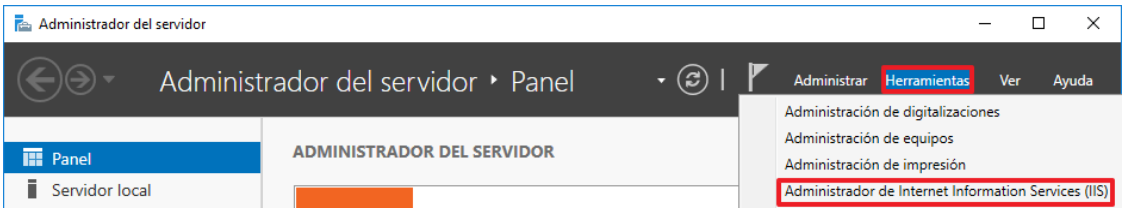
Paso	Descripción
95.	La siguiente pantalla muestra la configuración, propiedades, por defecto.  **Nota:** Tenga en cuenta que el registro administrativo se llenará, en condiciones normales, antes que el operacional.
96.	Para evitar, que una vez completado el fichero de registro, se empiece a borrar por 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”.
97.	Con la configuración dejada, 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”. Y el fichero de auditoría se vacía y comienza a llenarse de nuevo. **Nota:** Estos ficheros deberán ser copiados y eliminados periódicamente para evitar su pérdida y el llenado del disco duro.

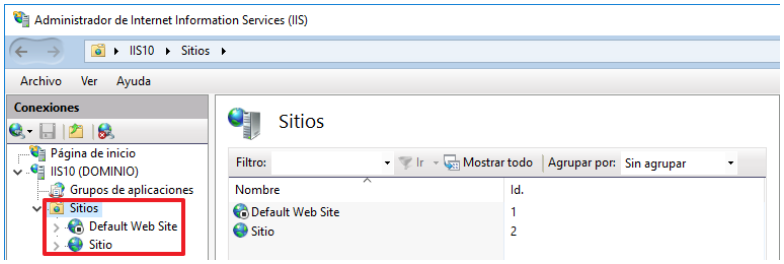
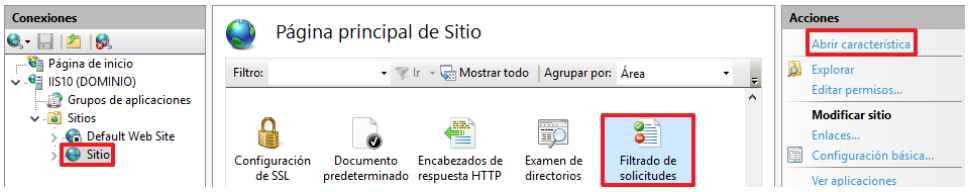
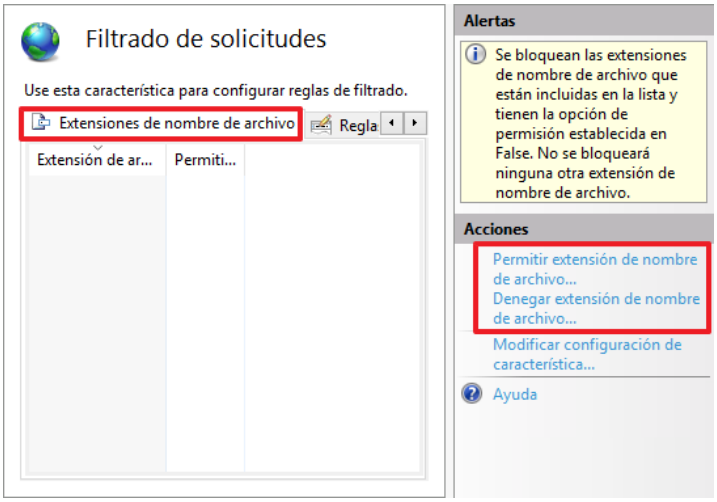
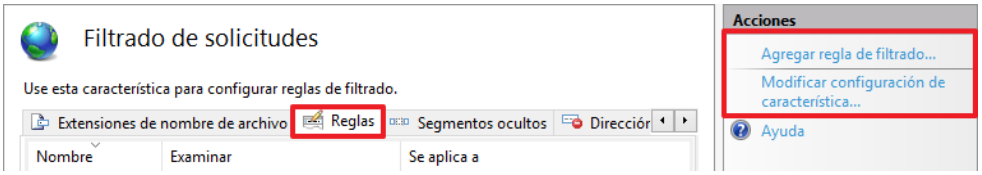
2.7. FILTRADO DE SOLICITUDES

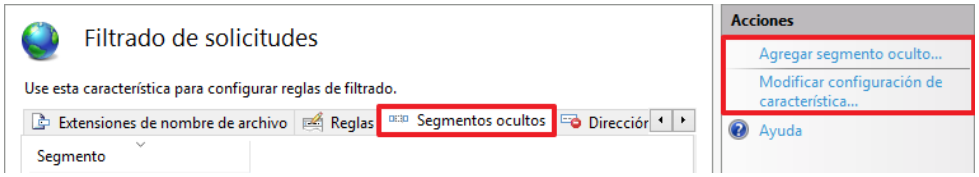
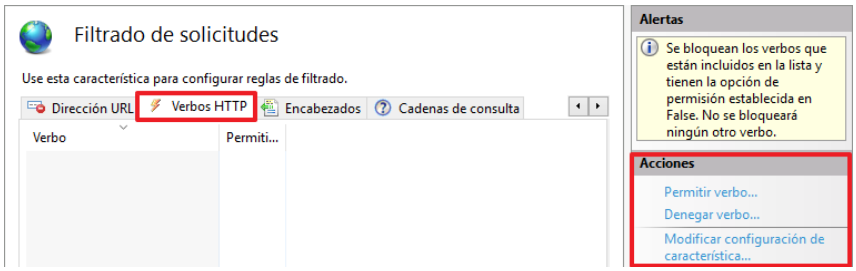
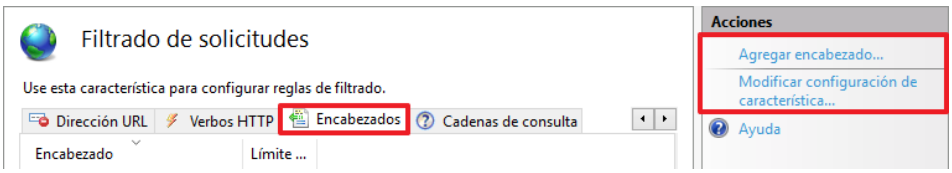
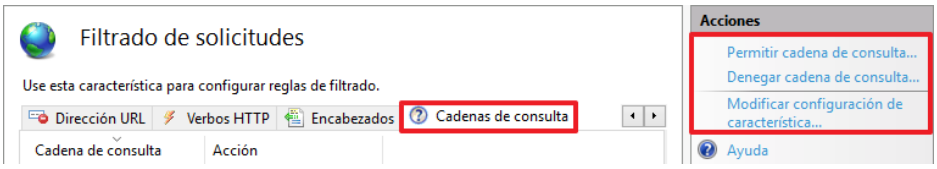
El siguiente paso define el procedimiento para la configuración del filtro de solicitudes el cual se encarga de analizar todas las solicitudes que entran en el servidor web y las filtra basándose en reglas establecidas previamente.

La mayoría de los ataques malintencionados comparten características comunes, como direcciones URL muy largas o solicitudes de una acción inusual, es por ello que filtrando las solicitudes se puede reducir el impacto de este tipo de ataques.

Cada organización debe determinar que extensiones son las específicamente necesarias para la funcionalidad del sitio web que tiene alojado y deberá configurar el filtro para soportar únicamente las extensiones exclusivamente necesarias.

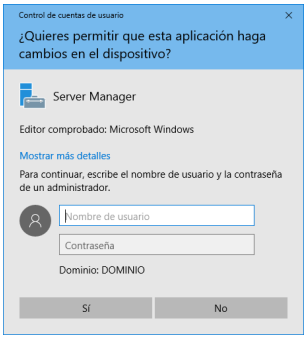
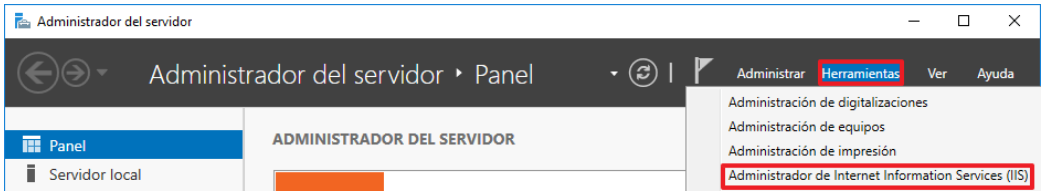
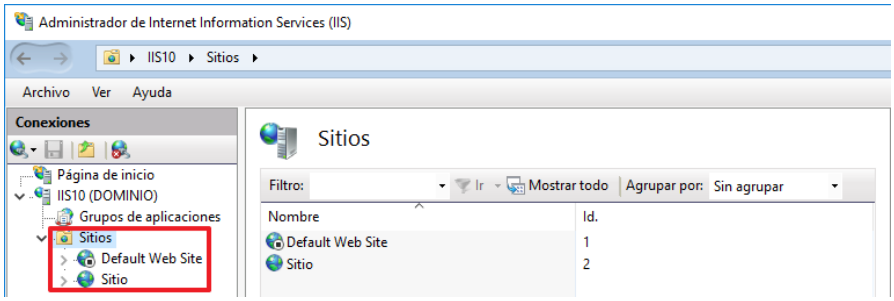
Paso	Descripción
98.	Inicie sesión en el servidor miembro donde tiene instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
99.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 
100.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”** 

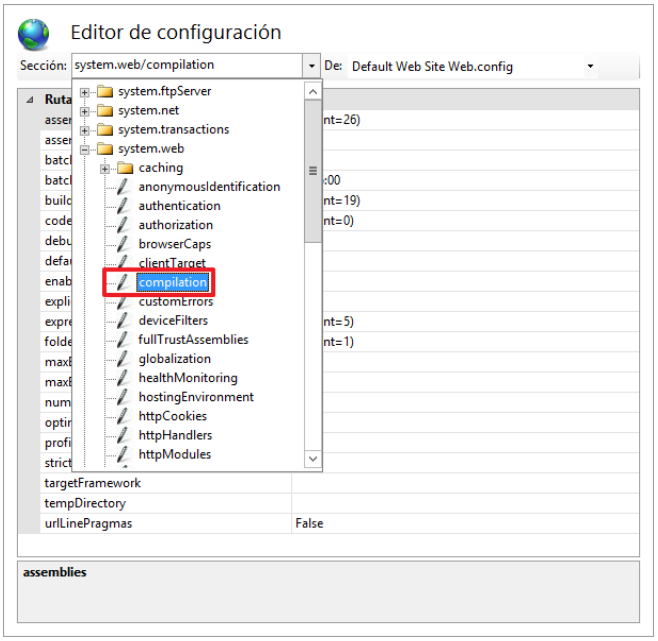
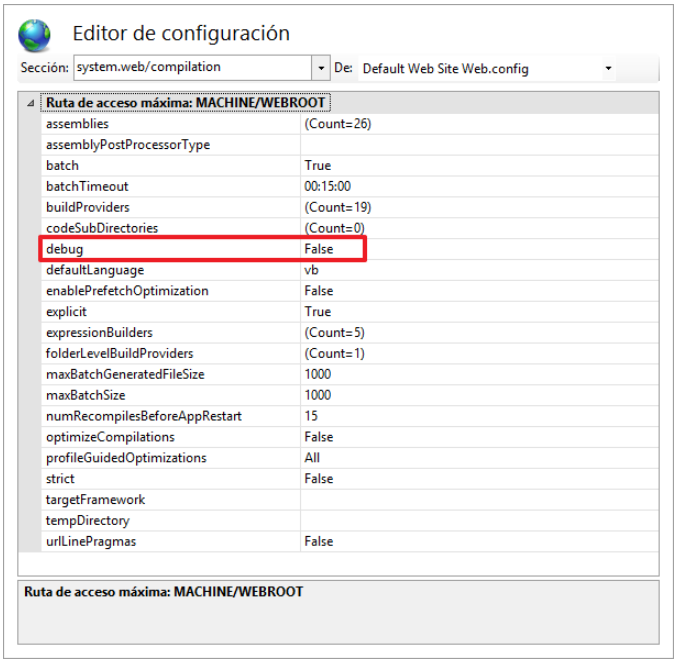
Paso	Descripción
101.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo de “Conexiones” y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.
102.	Seleccione en la página principal del sitio web el icono “Filtrado de solicitudes” y pulse sobre “Abrir característica” sitiado en el menú acciones del panel superior derecho de la pantalla. 
103.	A continuación, en la pestaña “Extensiones de nombre de archivo” puede permitir o denegar extensiones. 
104.	En la pestaña “Reglas” puede agregar o modificar reglas de filtrado. 

Paso	Descripción
105.	En la siguiente pestaña puede agregar o modificar segmentos ocultos. 
106.	En la siguiente pestaña puede permitir, denegar o modificar direcciones URL. 
107.	En la siguiente pestaña puede permitir, denegar o modificar Verbos. 
108.	En la siguiente pestaña puede agregar o modificar encabezados. 
109.	En la última pestaña puede permitir, denegar o modificar cadenas de consulta. 

2.8. DESHABILITAR MODOS DE DEPURACIÓN

El siguiente paso define el procedimiento para la modificación del fichero web.config para inhabilitar el modo de depuración de una aplicación en entornos de producción, evitando con ello posibles fisuras de seguridad.

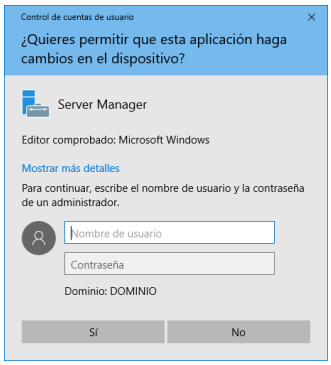
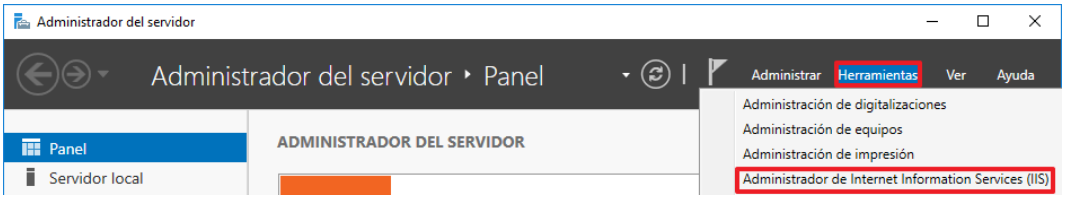
Paso	Descripción
110.	Inicie sesión en el servidor miembro donde tiene instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
111.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 
112.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”** 
113.	Localice el sitio web que desea configurar y seleccione “Editor de configuración”, a continuación, pulse en el menú “Acciones” la opción “Abrir característica” situado en la parte superior derecha de la pantalla para abrir el editor de configuración. 

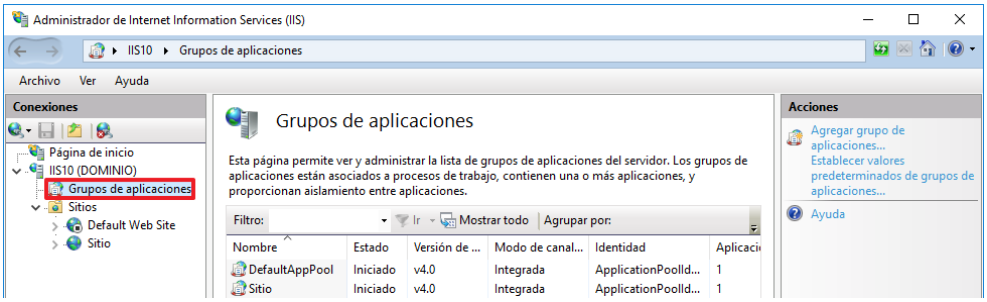
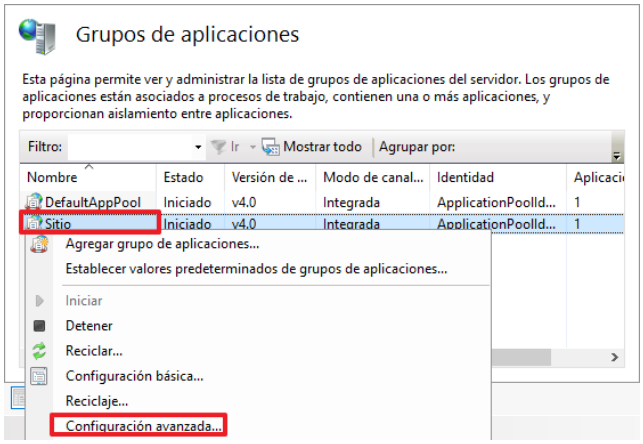
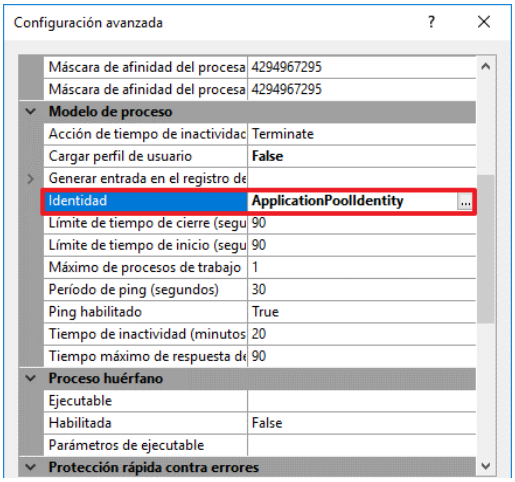
Paso	Descripción
114.	Navegue en “Sección” hasta “system.web/compilation”. 
115.	Localice la opción “Debug”, abra el desplegable y seleccione “False”. 

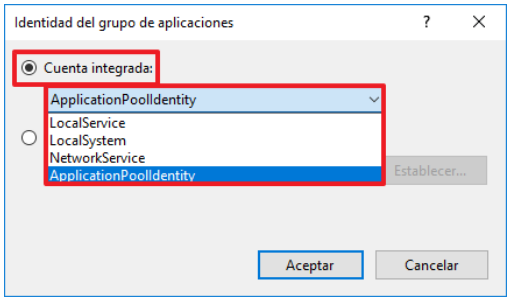
2.9. IDENTIDADES DEL GRUPO DE APLICACIONES

El siguiente paso define el procedimiento para la modificación de las identidades de una aplicación las cuales deben modificarse con la aplicación del ENS para la categoría alta sobre IIS 10 y evitando el uso de identidades de servicio integradas tales como servicio local o sistema local.

Para una mayor seguridad los grupos de aplicaciones deben ejecutarse bajo la identidad del grupo cuando se crea el grupo de aplicaciones, el valor predeterminado y más seguro es "ApplicationPoolIdentity". El uso de una cuenta personalizada es aceptable, pero debe asegurarse de usar una cuenta diferente para cada grupo de aplicaciones.

Paso	Descripción
116.	Inicie sesión en el servidor miembro donde tiene instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
117.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 
118.	Inicie la herramienta "Administrador de Internet Information Services (IIS)". Para ello, pulse sobre el menú superior de la derecha de la herramienta "Administrador del servidor" y seleccione **"Herramientas → Administrador de Internet Information Services (IIS)"** 

Paso	Descripción
119.	Despliegue el servidor y seleccione la opción “Grupos de aplicaciones”. 
120.	A continuación, seleccione la aplicación que desea configurar y haga clic botón derecho sobre ella y pulse “Configuración avanzada…”. 
121.	Localice la opción “Identidad” dentro de “Modelo de proceso”. 

Paso	Descripción
122.	A continuación, seleccione la opción que más se adecue a sus necesidades y pulse “Aceptar”. 

2.10. LIMPIEZA DE METADATOS

Se ha de tener en consideración que en un servidor web se pueden alojar documentos que pueden contener información oculta en los metadatos los cuales contienen información que permite catalogar, ordenar y clasificar nuestros archivos, por lo que pueden ser un riesgo de seguridad para nuestra organización, por lo que hay que tener especial atención en la limpieza de los metadatos de los documentos que se alojan en el servidor web por ello antes de alojar un fichero en el servidor web se ha debido de realizar el procedimiento indicado en MP. INFO. 6. LIMPIEZA DE DOCUMENTOS.

En el proceso de limpieza se ha de tener en consideración que se retiraran todos los datos de los documentos además de la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, con la excepción de la información pertinente para el receptor del documento.

2.11. SOLUCIONES WAF (WEB APLICATION FIREWALL)

Un servidor web puede alojar aplicaciones por lo que es importante un control exhaustivo de estas por ello se han de emplear uno de los elementos principales en la protección de entornos de aplicaciones Web que son los cortafuegos (firewalls) de aplicaciones Web, también conocidos como WAF, Web Application Firewall.

El WAF se encargará de proteger los servidores de aplicaciones web de determinados ataques específicos en Internet además de controlar las transacciones al servidor web de nuestra organización.

Este sistema nos permite evitar probables ataques como:

a) “Cross-site scripting” que consiste en la inclusión de código script malicioso en el cliente que consulta el servidor web.

b) “SQL injection” que consiste en introducir un código SQL que vulnere la Base de Datos de nuestro servidor.

c) “Denial-of-service” que consiste en que el servidor de aplicación sea incapaz de servir peticiones correctas de usuarios.

Algunos sistemas WAF existentes en el mercado también monitorizan las respuestas del servidor, por ejemplo, si en una respuesta, que el servidor web envía al usuario se detectan cadenas que pueden ser identificadas como cuentas bancarias, el WAF lo puede detectar como un posible ataque y denegar la respuesta.

3. GESTIÓN DE ROLES Y/O CARACTERÍSTICAS DEL SISTEMA

Estos paso a paso se deberán aplicar para instalar o desinstalar roles y/o características implementadas en un servidor miembro del dominio, que le sea de aplicación la guía de securización "CCN-STIC-570A - Implementación del ENS en Microsoft Windows Server 2016" a partir de la categoría media del ENS.

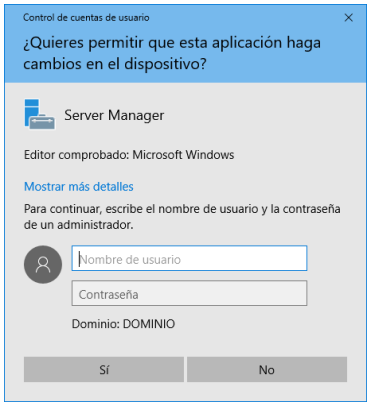
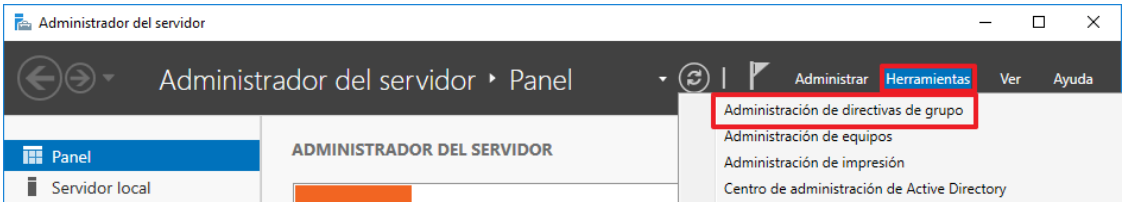
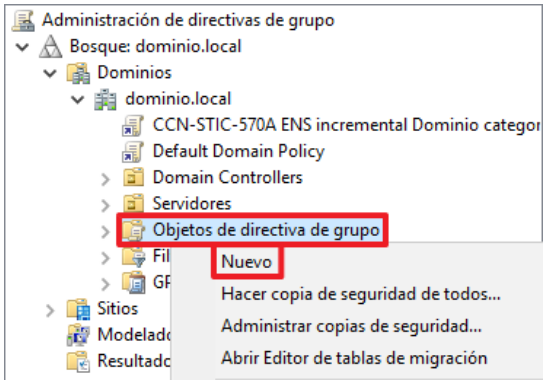
3.1. PREPARACIÓN DEL DIRECTORIO ACTIVO

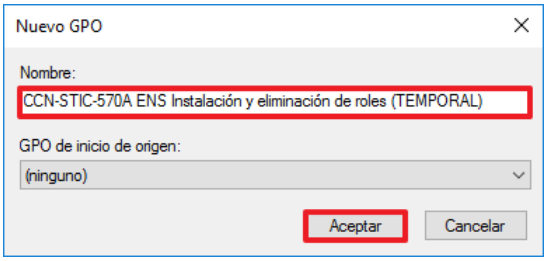
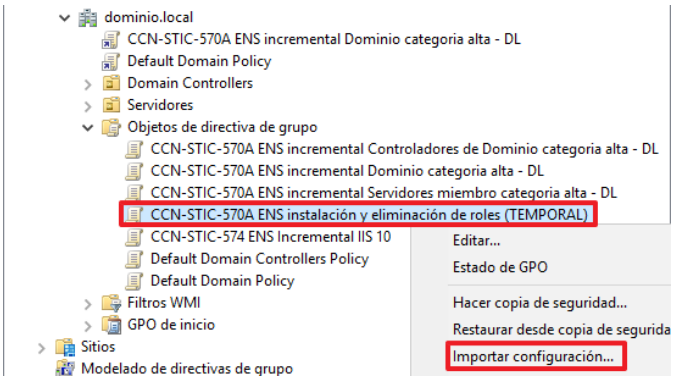
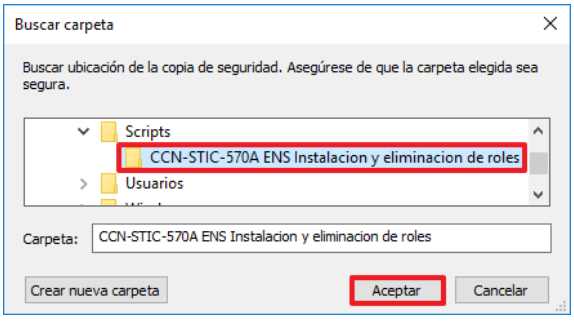
Para instalar o eliminar un rol y/o característica será necesario la creación de una política de seguridad temporal para tal efecto.

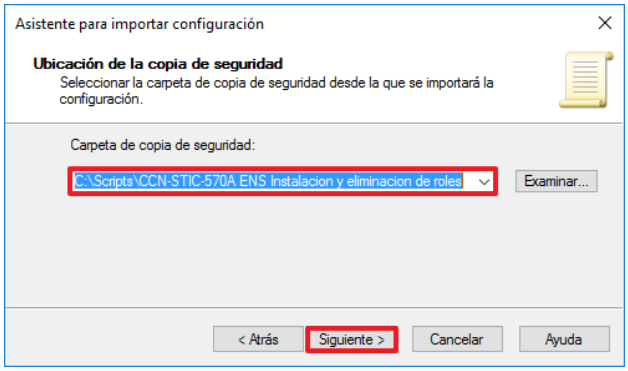
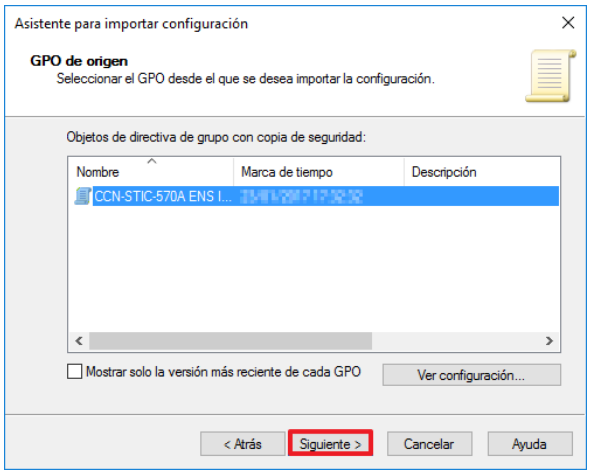
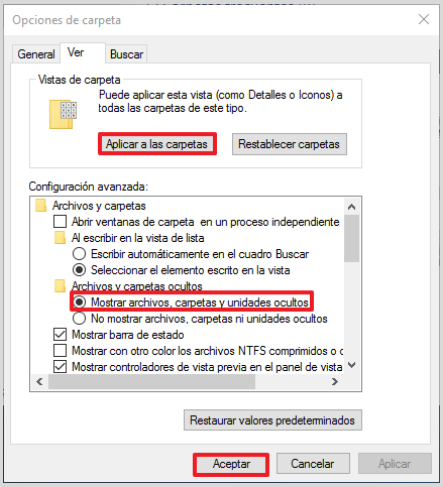
Los pasos que se describen a continuación se realizarán en un controlador de dominio del directorio activo al que va a pertenecer el servidor miembro que se está securizando.

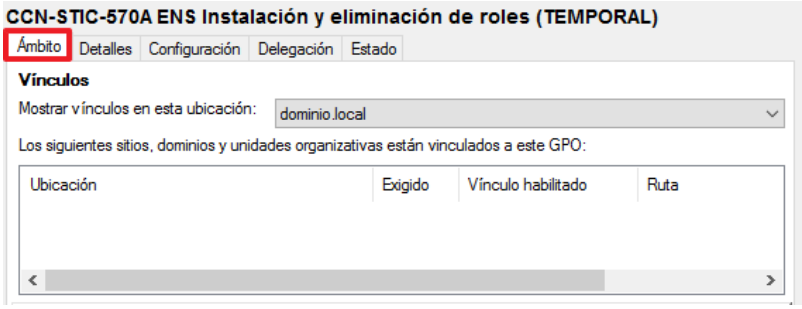
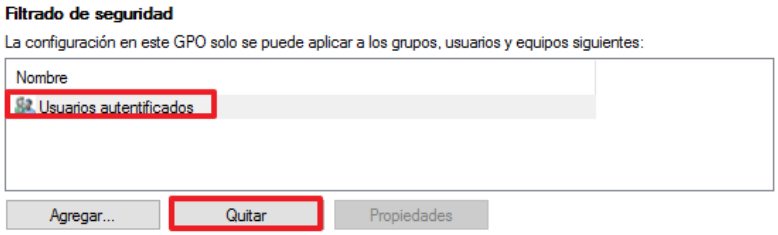
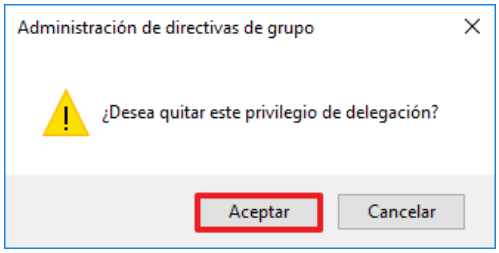
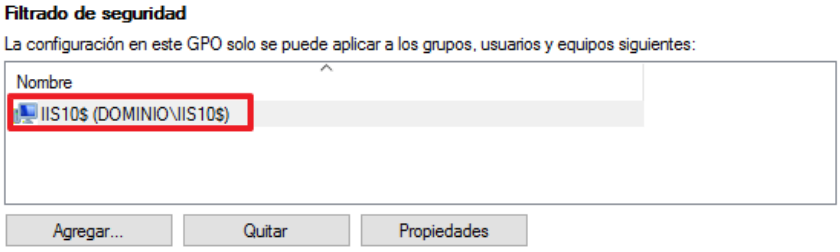
Nota: Recuerde que una vez instalados o eliminados los roles y/o características necesarias deberá aplicar el paso "3.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO".

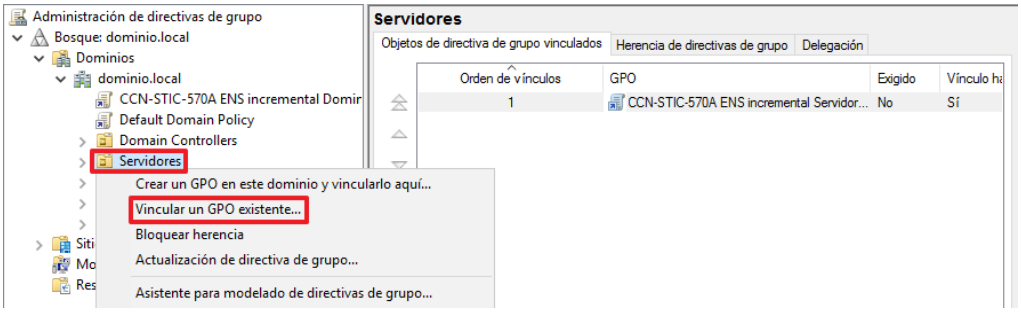
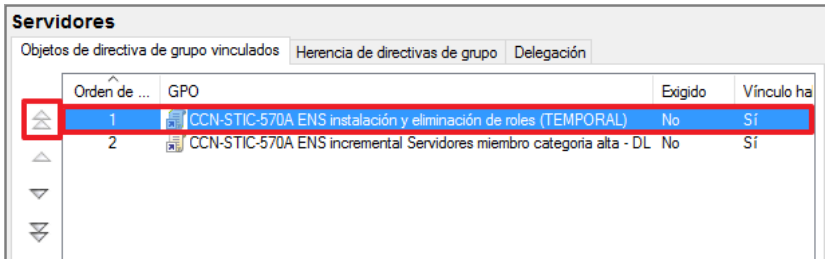
Paso	Descripción
123.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
124.	Cree el directorio "Scripts" en la unidad "C:\". **Nota:** Los scripts asumen que su ubicación en el sistema será bajo "C:\Scripts". Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
125.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".
126.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 

Paso	Descripción
127.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Si”. 
128.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”** 
129.	Ubíquese sobre el nodo “Objetos de directiva de grupo” ubicado en **“Bosque:<su dominio> → Dominios → <su dominio> → Objetos de directiva de grupo”**.
130.	Si ya estuviese creada la directiva de grupo “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)” deberá continuar a partir del paso 141.
131.	Pulse con el botón derecho, sobre dicha carpeta y seleccione la opción “Nuevo”. 

Paso	Descripción
132.	Introduzca como nombre “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)” y pulse el botón “Aceptar”. 
133.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración…”. 
134.	En el asistente de importación de configuración, pulse el botón “Siguiente >”.
135.	En “Carpeta de copia de seguridad”, pulse el botón “Examinar...”.
136.	Seleccione la carpeta “CCN-STIC-570A ENS Instalación y eliminación de roles” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 

Paso	Descripción
137.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada. 
138.	Compruebe que aparece la política de seguridad “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)” y pulse el botón “Siguiente >”.  **Nota:** Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero “manifest.xml”. Este es un fichero oculto y, por lo tanto, debe mostrar en “opciones de carpeta” la opción “Mostrar archivos, carpetas y unidades ocultos”. 

Paso	Descripción
139.	En la pantalla de examen, pulse el botón “Siguiente >”.
140.	Para completar el asistente pulse el botón “Finalizar”.
141.	A continuación, seleccione la nueva política de grupo configurada y diríjase a la pestaña “Ámbito” que se encuentra en el panel derecho. 
142.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
143.	A continuación, pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
144.	Una vez quitado, pulse el botón “Agregar…” y seleccione únicamente los equipos o grupos sobre los que desea aplicar la política de seguridad  **Nota:** En este ejemplo se agrega el equipo IIS10.

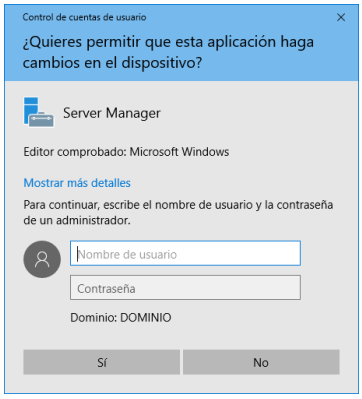
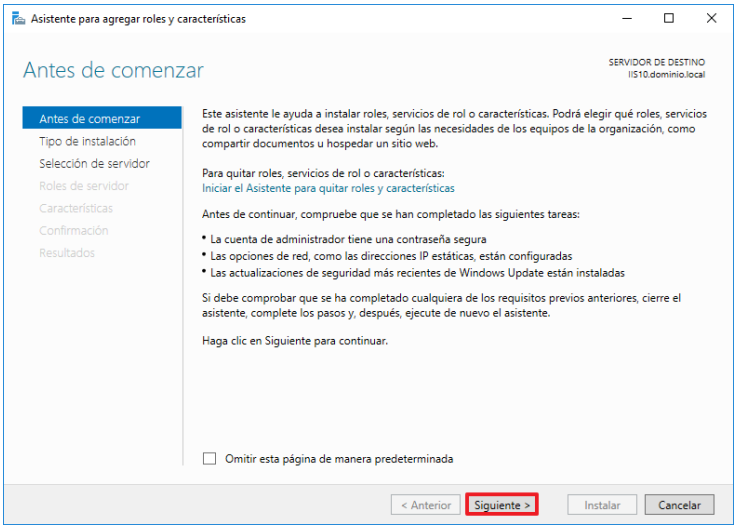
Paso	Descripción
145.	A continuación, identifique las unidades organizativas en la que desea instalar o eliminar algún rol y/o característica. Pulse con el botón derecho sobre la unidad organizativa deseada y seleccione la opción del menú contextual “Vincular un GPO existente…”.  **Nota:** En este ejemplo se selecciona la unidad organizativa “Servidores”.
146.	Una vez vinculado, en el panel derecho seleccione la pestaña “Objetos de directiva de grupo vinculados” y seleccione la política “CCN-STIC 570A ENS Instalación y eliminación de roles”
147.	Pulse el botón con la flecha que apunta hacia arriba hasta situar la política “CCN-STIC 570A ENS Instalación y eliminación de roles” en primer lugar dentro del orden de vinculación. 

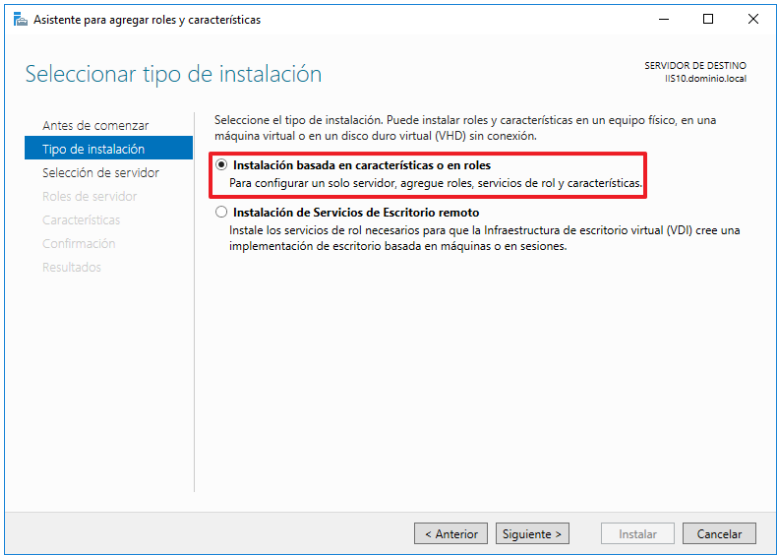
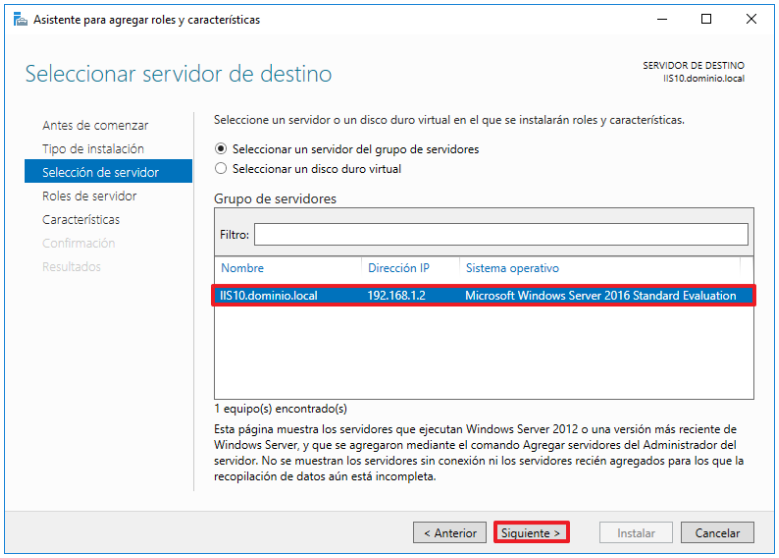
3.2. INSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS

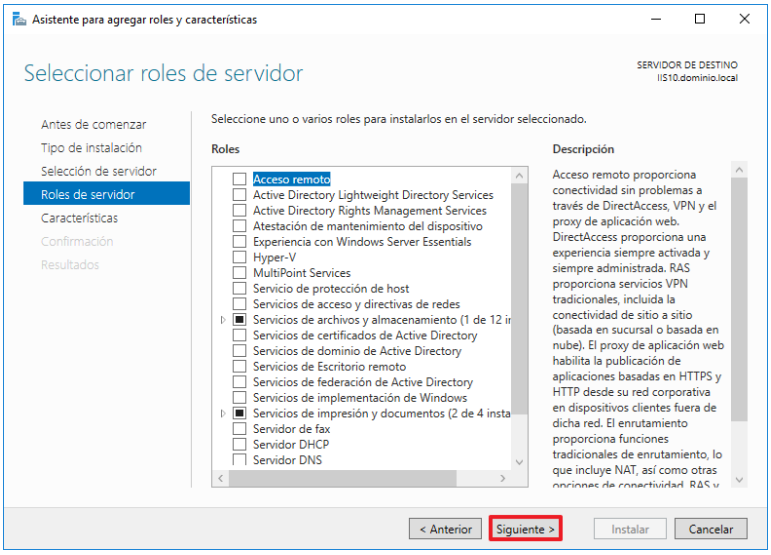
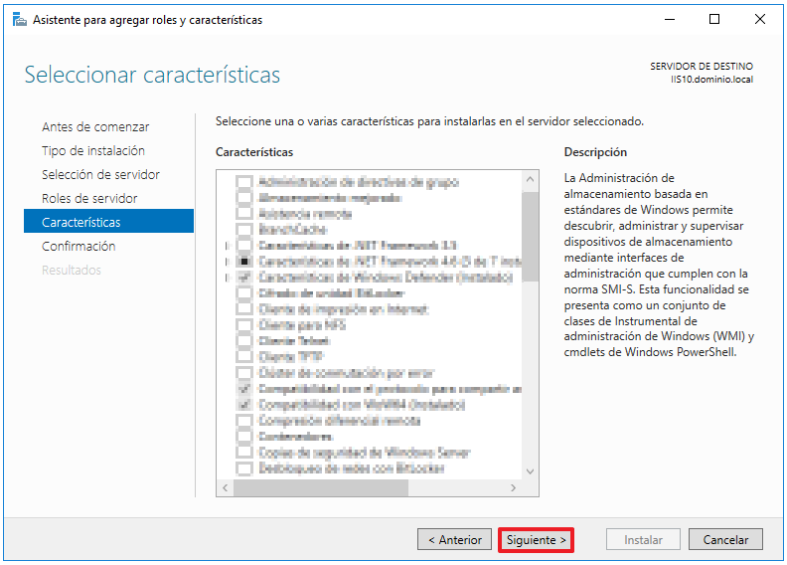
Los pasos que se describen a continuación se realizarán en el servidor miembro del dominio que se está securizando.

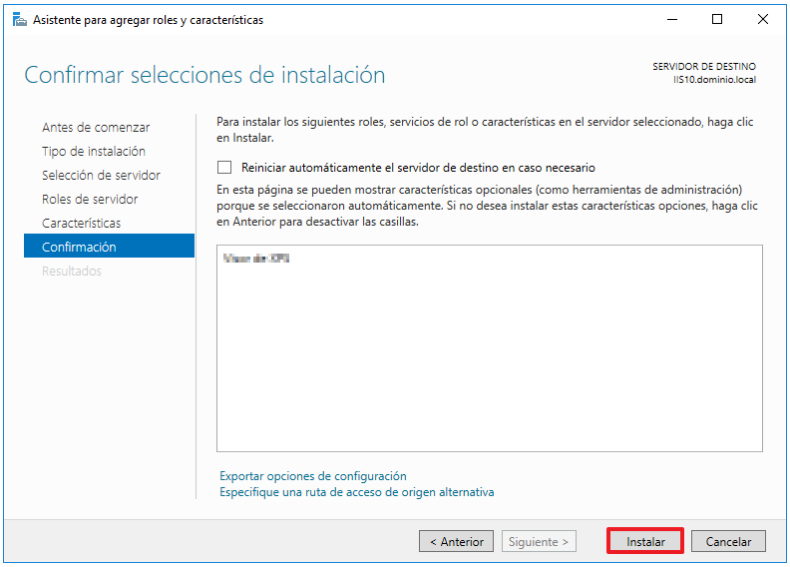
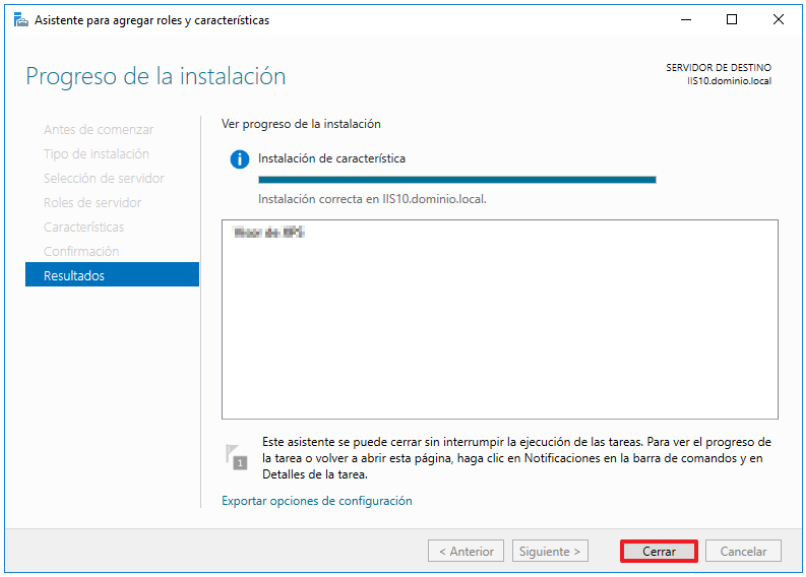
Nota: Para continuar este paso a paso debe haber aplicado previamente el punto “3.1 PREPARACIÓN DEL DIRECTORIO ACTIVO”.

Paso	Descripción
148.	Inicie sesión en el servidor miembro donde vaya a instalar un rol y/o característica. **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.

Paso	Descripción
149.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
150.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
151.	A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Agregar roles y características”. 
152.	Comenzará el asistente para agregar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 

Paso	Descripción
153.	Seleccione el tipo de instalación, “Instalación basada en características o roles” y pulse “Siguiente >” para continuar. 
154.	Seleccione el servidor sobre el cual desea instalar un rol o una característica, y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “IIS10”.

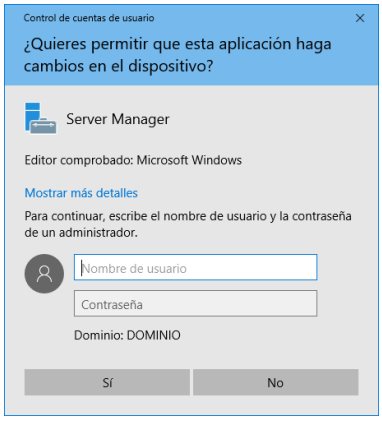
Paso	Descripción
155.	En la siguiente ventana, seleccione los roles que desee instalar en el sistema y pulse “Siguiente >”. 
156.	A continuación, en la siguiente ventana podrá seleccionar las características que desee instalar en el sistema. Seleccione aquellas que desee instalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se instala una característica de prueba, deberá adaptar este paso a los requerimientos de su organización.

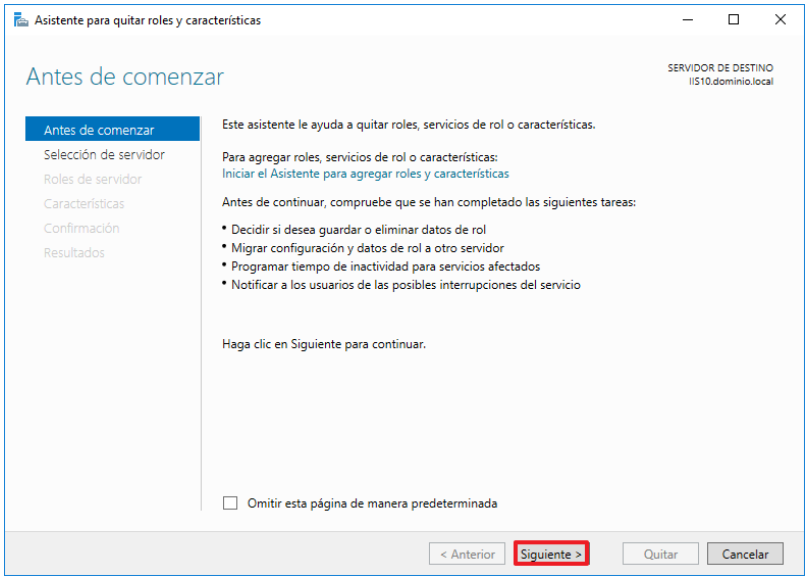
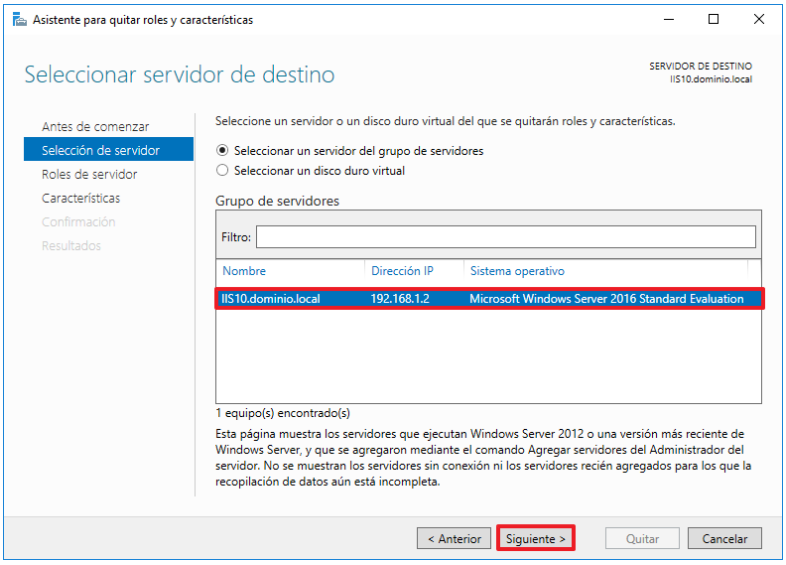
Paso	Descripción
157.	En la ventana “Confirmación” pulse “Instalar” para iniciar el proceso. 
158.	Una vez finalizado el proceso de instalación, pulse sobre “Cerrar” para finalizar la instalación.  **Nota:** En caso de ser necesario, el servidor requerirá un reinicio para finalizar la instalación de roles y características.
159.	Una vez finalizada la instalación de roles y/o características, deberá aplicar el siguiente paso “3.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

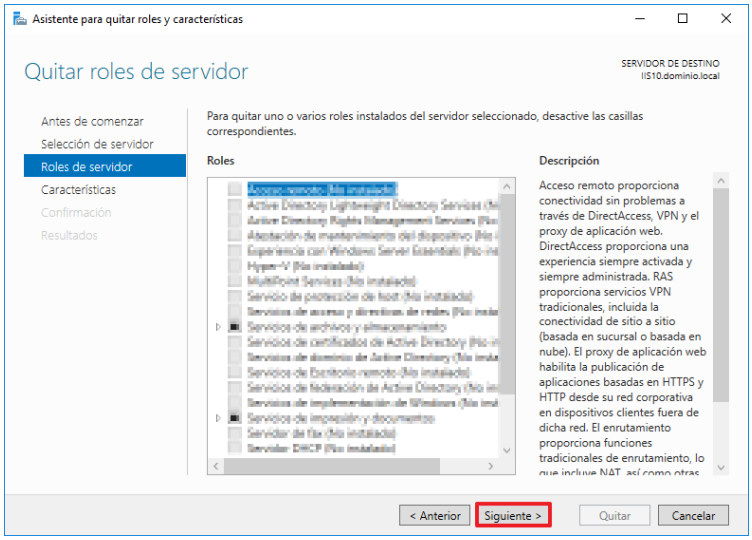
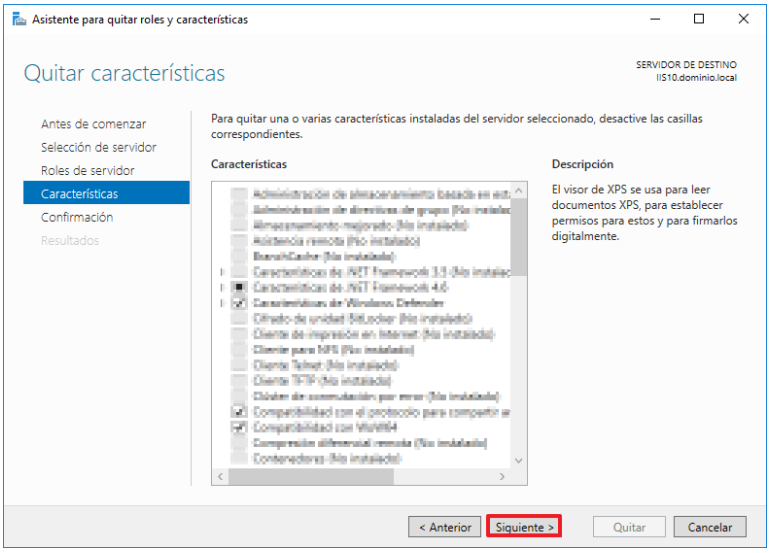
3.3. DESINSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS

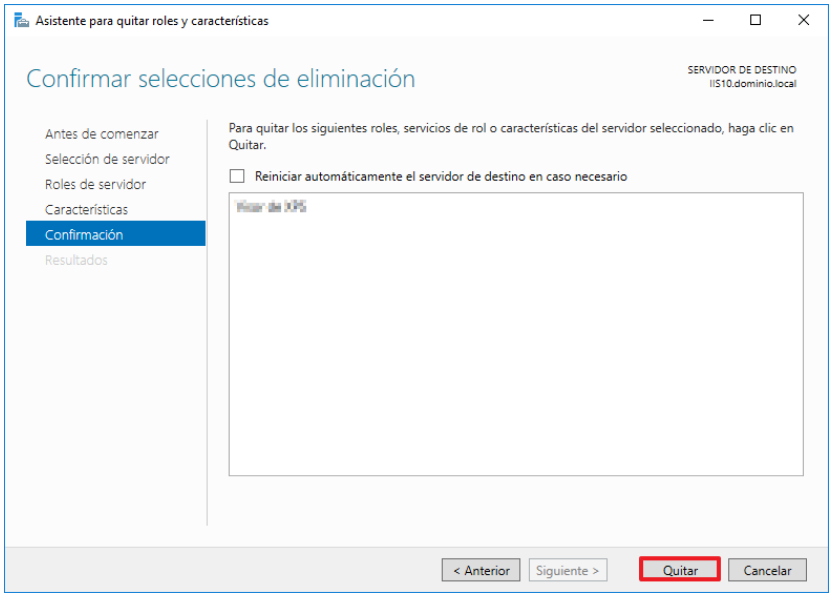
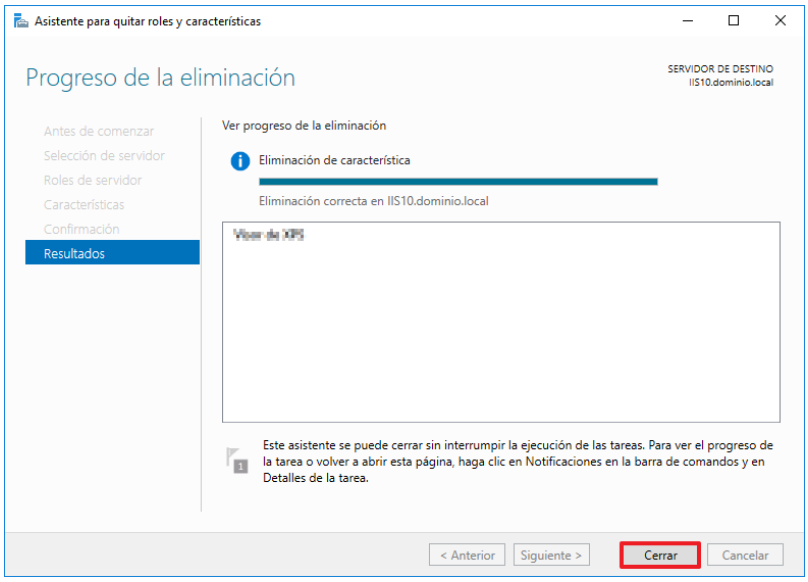
Los pasos que se describen a continuación se realizarán en el servidor miembro del dominio que se está securizando.

Nota: Para continuar este paso a paso debe haber aplicado previamente el punto "3.1 PREPARACIÓN DEL DIRECTORIO ACTIVO".

Paso	Descripción
160.	Inicie sesión en el servidor miembro donde vaya a eliminar un rol y/o característica.  **Nota:** Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.
161.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
162.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Si". 
163.	A continuación, pulse sobre el botón "Administrar" y seleccione la opción "Quitar roles y funciones". 

Paso	Descripción
164.	Comenzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 
165.	Seleccione el servidor sobre el cual desea eliminar un rol o una característica y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “IIS”.

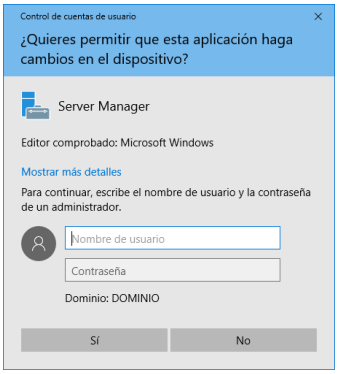
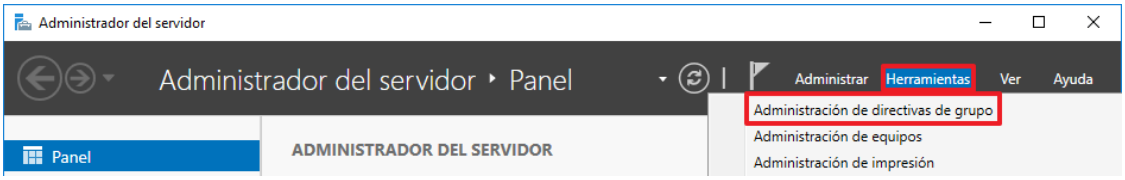
Paso	Descripción
166.	En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Seleccione aquellos que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo no se desinstala ningún rol, deberá adaptar este paso a los requerimientos de su organización.
167.	A continuación, en la siguiente ventana podrá seleccionar las características que desee desinstalar del sistema. Desmarque aquellas que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se desinstala una característica de prueba, deberá adaptar este paso a los requerimientos de su organización.

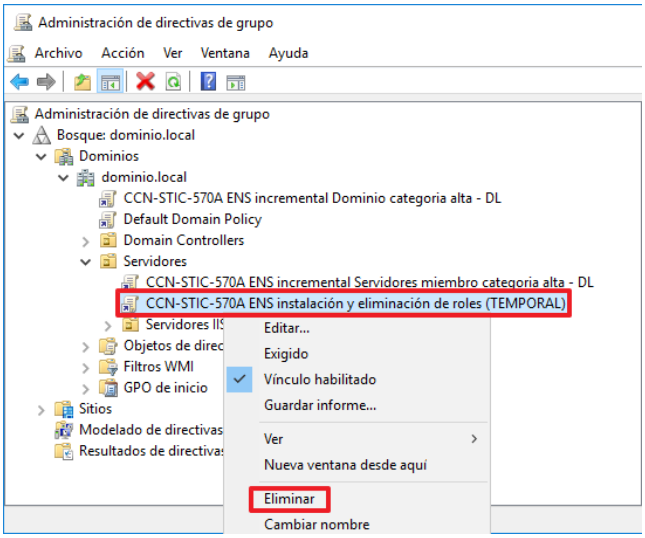
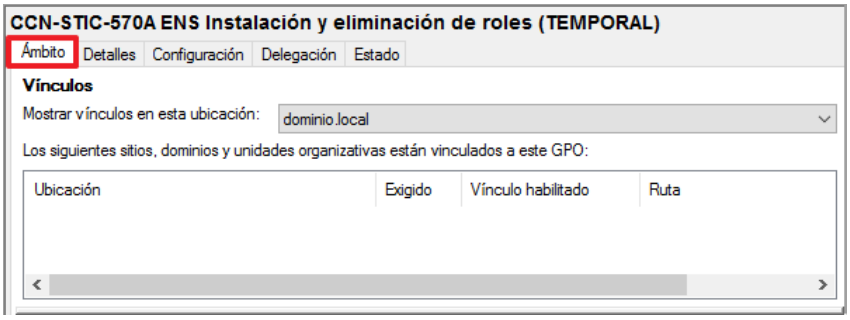
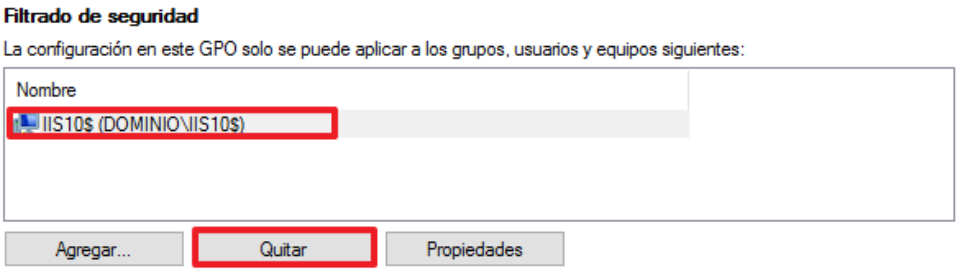
Paso	Descripción
168.	En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso. 
169.	Una vez finalizado el proceso de desinstalación, pulse sobre “Cerrar” para finalizar la desinstalación.  **Nota:** En caso de ser necesario el servidor requerirá un reinicio para finalizar la desinstalación de roles y características.
170.	Una vez finalizada la desinstalación de roles y/o características, deberá aplicar el siguiente paso “3.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

3.4. DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO

Para desvincular o eliminar la GPO “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)” creada en el paso “3.1 PREPARACIÓN DEL DIRECTORIO ACTIVO” deberá implementar el siguiente paso a paso.

Los pasos que se describen a continuación se realizarán en un controlador de dominio del domino al que va a pertenecer el servidor miembro que se está securizando.

Paso	Descripción
171.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
172.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
173.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Si”. 
174.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”** 

Paso	Descripción
175.	Localice la unidad organizativa donde se está aplicando la GPO “CCN-STIC-570A ENS Instalación o eliminación de roles (TEMPORAL)”.
176.	Pulse botón derecho sobre la GPO y seleccione la opción del menú contextual “Eliminar”. 
177.	A continuación, seleccione la política de grupo “CCN-STIC-570A ENS Instalación y eliminación de roles (TEMPORAL)” ubicada en el contenedor “Objetos de directiva de grupo” y diríjase a la pestaña “Ámbito” que se encuentra en el panel derecho. 
178.	En la opción “Filtrado de seguridad”, Seleccione los equipos o grupos sobre los que se está aplicando la política de seguridad y pulse sobre el botón “Quitar”.  **Nota:** En este ejemplo se elimina el equipo “IIS10”

ANEXO A.4.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA PARA SERVIDORES IIS 10 SOBRE MICROSOFT WINDOWS SERVER 2016 EN ENTORNO DE DOMINIO

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores IIS 10 sobre Microsoft Windows Server 2016 con implementación de seguridad de categoría alta del ENS / Difusión Limitada.

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

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar la sección de la guía "ANEXO A.4.1 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 MIEMBROS DE DOMINIO SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS/DIFUSIÓN LIMITADA".

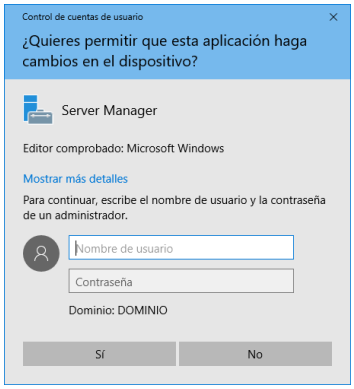
1. COMPROBACIONES EN CONTROLADOR DE DOMINIO

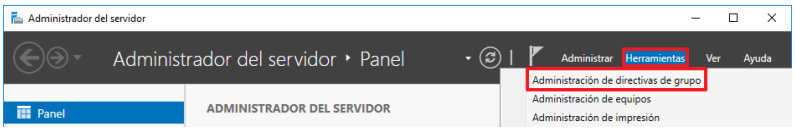
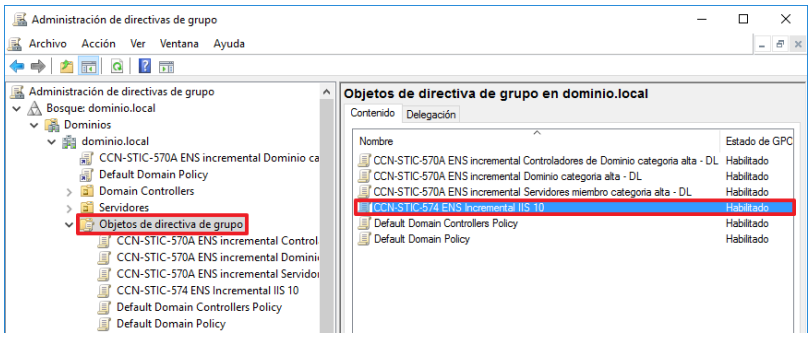
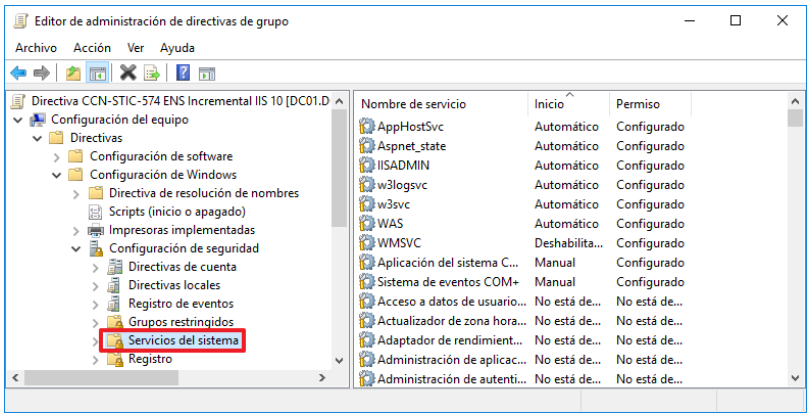
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador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

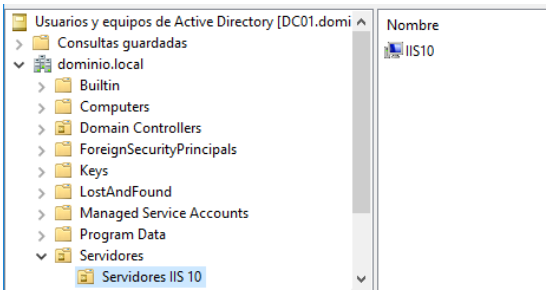
a) Usuarios y equipos de Active Directory (dsa.msc).

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

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

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio.		Inicie sesión con una cuenta que tenga privilegios de administración del dominio. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Introduzca credenciales de administrador y pulse "Sí" en la ventana de "Control de cuentas de usuario". 

Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que los objetos de directivas de grupo han sido creados y están habilitados.		Ejecute la herramienta "Administrador de directivas de grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Administración de directivas de grupo"**  Dentro de la consola diríjase a los "Objetos de directiva de grupo": "**Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo**" Verifique que están creados los tres objetos de directiva de grupo "CCN-STIC-574 ENS Incremental IIS 10", y que en la columna "Estado de GPO" figuran como habilitadas. 
3. Verifique los valores de los servicios del sistema de la directiva CCN-STIC-574 ENS Incremental IIS 10		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-574 ENS Incremental IIS 10" tiene los siguientes valores de servicios de sistema dentro de: **"Directiva CCN-STIC-574 ENS Incremental IIS 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"**. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="4">Cómo hacerlo</th></tr>
<tr><th colspan="2">Servicio (nombre largo)</th><th>Servicio (nombre corto)</th><th>Inicio</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td colspan="2">Servicio auxiliar de host para aplicaciones</td><td>AppHostSvc</td><td>Automático</td><td></td><td></td></tr>
<tr><td colspan="2">ASP.NET State Service</td><td>Aspnet_state</td><td>Automático</td><td></td><td></td></tr>
<tr><td colspan="2">Aplicación del sistema COM+</td><td>COMSysApp</td><td>Manual</td><td></td><td></td></tr>
<tr><td colspan="2">Servicio de administración IIS</td><td>IISADMIN</td><td>Automático</td><td></td><td></td></tr>
<tr><td colspan="2">Servicio de registro de W3C</td><td>w3logsvc</td><td>Automático</td><td></td><td></td></tr>
<tr><td colspan="2">Servicio de publicación World Wide Web</td><td>w3svc</td><td>Automático</td><td></td><td></td></tr>
<tr><td colspan="2">Servicio WAS</td><td>WAS</td><td>Automático</td><td></td><td></td></tr>
<tr><td colspan="2">Servicio de Administración Web</td><td>WMSVC</td><td>Manual</td><td></td><td></td></tr>
<tr><td>4. Verifique que los servidores de IIS 10 están dentro de las Unidades Organizativas correspondientes</td><td></td><td colspan="4">Utilice la herramienta Usuarios y equipos de Active Directory (“Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory”) y seleccione las unidades organizativas que contienen los Servidores IIS 10.
Nota: Para el desarrollo de esta guía se utiliza la Unidad Organizativa “Servidores IIS 10”.
 
</td></tr>
</table>

2. COMPROBACIONES EN SERVIDOR MIEMBRO

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

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

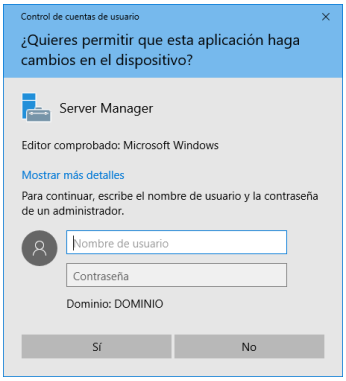
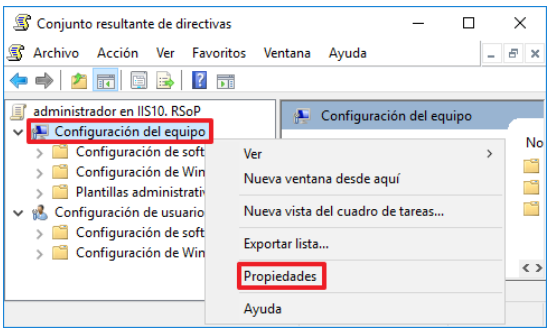
a) Administrador del Servidor

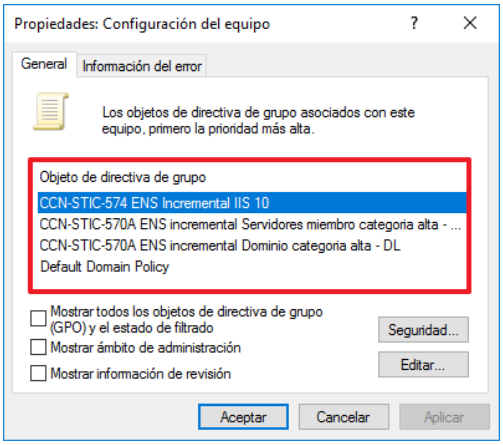
b) Conjunto resultante de directivas (rsop.msc)

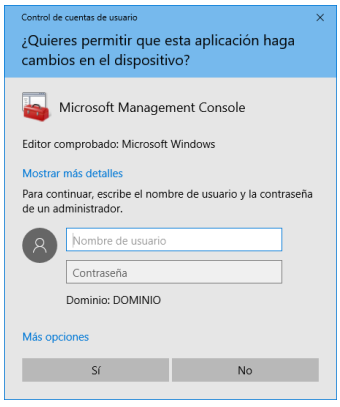
c) Consola de servicios (services.msc)

d) Editor de registro (regedit.exe)

e) Explorador de Archivos (explorer.exe)

Comprobación	OK/NOK	Cómo hacerlo
5. Inicie sesión en el servidor a comprobar.		En uno de los servidores miembro del dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Introduzca credenciales de administrador y pulse "Sí" en la ventana de control de cuentas de usuario. 
6. Verifique que el equipo ha recibido la directiva de grupo CCN-STIC-574 ENS incremental IIS 10.		Ejecute la consola de administración "Conjunto resultante de directivas" (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → rsop.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse "Sí". Seleccione en ella la rama "Configuración del equipo", márquela con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la figura. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td></td><td></td><td>En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", resaltada en la siguiente figura.
 

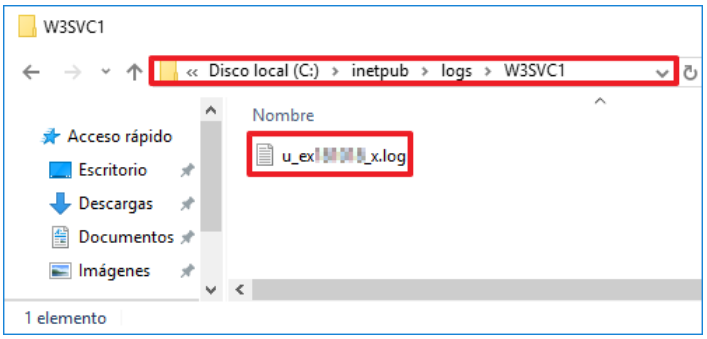
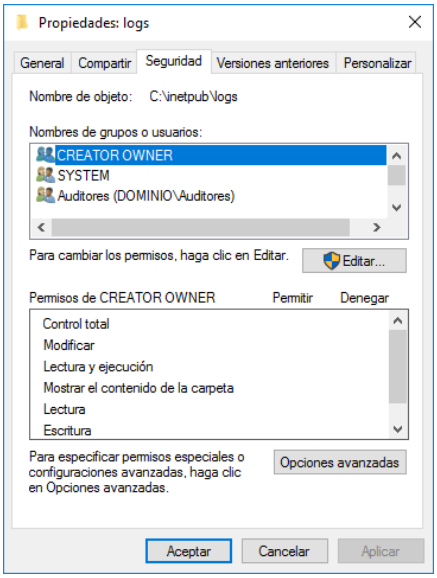
Verifique que en dicha sección aparecen listados, y por ese orden, los objetos de directiva de grupo que se indican en la siguiente tabla:
<table>
<tr><th>Objeto de directiva de grupo</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-574 ENS incremental IIS 10</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS incremental Servidores miembro categoria alta - DL</td><td></td></tr>
<tr><td>CCN-STIC-570A ENS incremental Dominio categoria alta – DL</td><td></td></tr>
<tr><td>Default Domain Policy</td><td></td></tr>
</table></td></tr>
<tr><td>7. Verifique que los servicios del sistema están correctamente configurados</td><td></td><td>Usando la consola de servicios (el sistema solicitará elevación de privilegios):
“Tecla Windows+R → services.msc”
El Control de cuentas de usuario solicitará elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse “Sí” para continuar.
 
</td></tr>
</table>

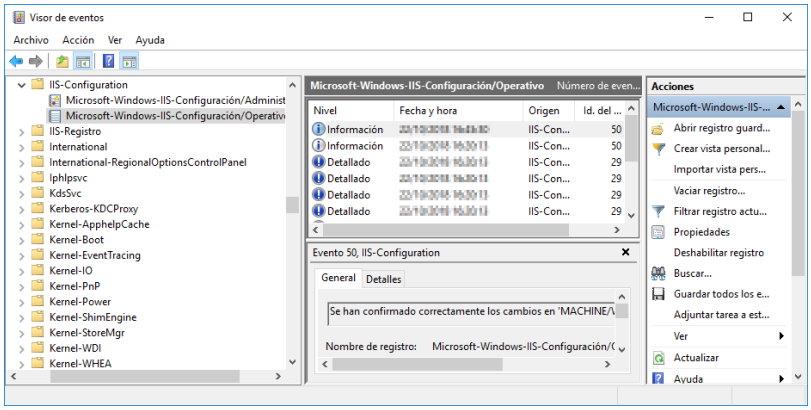
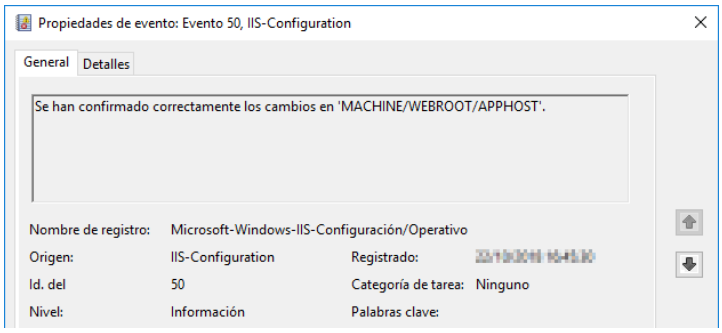
Comprobación	OK/NOK	Cómo hacerlo
		Verifique que el tipo de inicio de los servicios que aparecen en el sistema y en la siguiente tabla coinciden. **Nota:** Dependiendo de las características de IIS 10 instaladas en el equipo es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales.

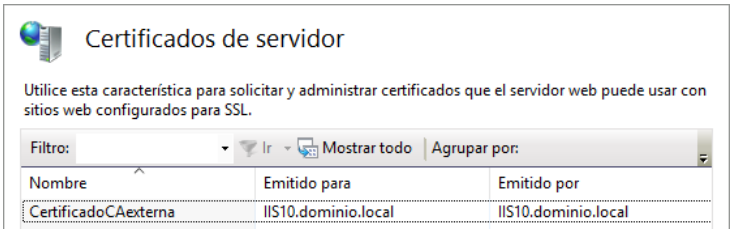
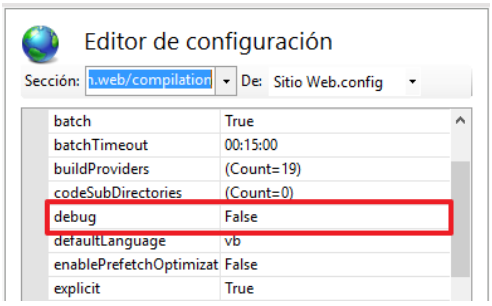
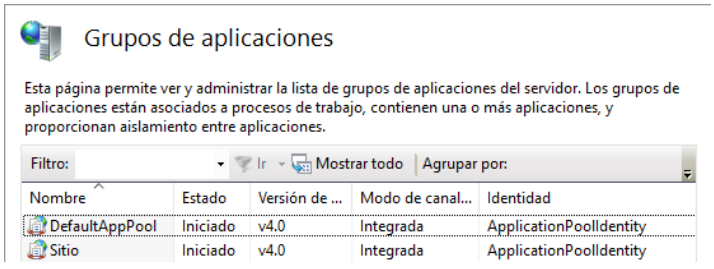
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio auxiliar de host para aplicaciones	AppHostSvc	Automático		
ASP.NET State Service	Aspnet_state	Automático		
Aplicación del sistema COM+	COMSysApp	Manual		
Servicio de administración IIS	IISADMIN	Automático		
Servicio de registro de W3C	w3logsvc	Automático		
Servicio de publicación World Wide Web	w3svc	Automático		
Servicio WAS	WAS	Automático		
Servicio de Administración Web	WMSVC	Manual		

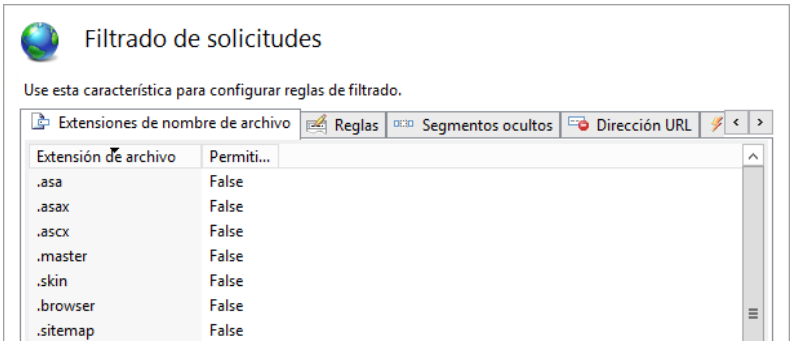
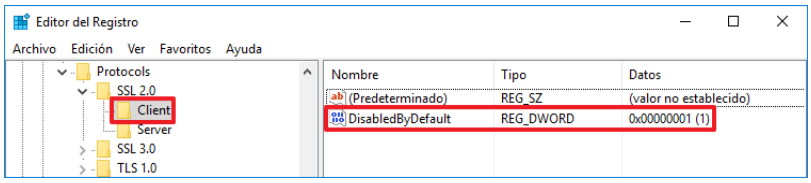
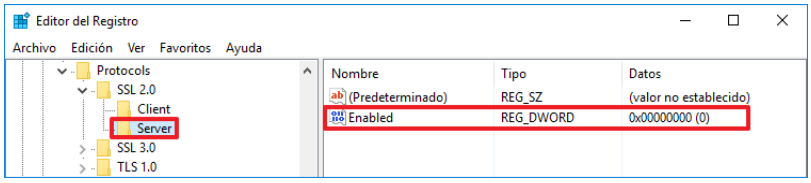
8. Verifique que se han asignado los permisos correctos en el sistema de archivos		Utilizando el Explorador de Windows: **"Windows+R → Explorer"** En caso de no saber dónde apunta cada una de las rutas abreviadas que se especifica, ejecute Explorer <<ruta>> donde <<ruta>> se sustituirá por la ruta abreviada. **Nota:** Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, marcándolo con el botón derecho y eligiendo la opción "Propiedades" del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá situarse en la pestaña "Seguridad". En la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios. Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados.

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\inetsrv\MetaBack	Administrador	Control total	
	System	Control total	
%SystemRoot%\LogFiles	Administrador	Control total	
	System	Control total	
	Creator Owner	Control total	

Comprobación	OK/NOK	Cómo hacerlo
9. Compruebe que el registro de acceso de IIS está operativo.		En la configuración que ha realizado ha habilitado el registro de acceso al servidor, por lo que debe asegurarse que está registrando la actividad. Para ello verifique que el directorio **E:\inetpub\logs\W3SVC1** contiene ficheros con el formato **u_ex*fecha*.log**. Abriendo el último deberá ver que registra los accesos correctamente.  **Nota:** Tenga en cuenta que no se crea ningún registro hasta que no se realiza alguna actividad.
10. Compruebe los permisos de la carpeta Logs		Compruebe los permisos de la carpeta Logs, únicamente los usuarios Auditores además del sistema deben tener acceso.  **Nota:** Si no dispone del grupo Auditores deberá crearlo previamente.

Comprobación	OK/NOK	Cómo hacerlo
11. Verifique que los registros de Windows están habilitados		Los registros de aplicaciones y servicios integrados con el sistema operativo deben estar habilitados y almacenando información. Abra el Visor de eventos y busque: **"Menú inicio → Herramientas administrativas → Visor de eventos → Registros de aplicaciones y servicios → Microsoft → Windows → IIS-Configuration"**.  Situándose sobre cada uno de ellos, abra el menú contextual, con el botón derecho del ratón, y compruebe que aparece la opción "Deshabilitar registro", lo cual indica que está habilitado.
12. Verifique que los registros son actuales.		Los dos registros deben contener eventos, abra ambos y compruebe que las últimas fechas de registro son recientes. 

Comprobación	OK/NOK	Cómo hacerlo
13. Comprobación certificado sitio web HTTPS		Dentro de la consola del "Administrador de Internet Information Services (IIS)" accedemos a "Certificados de servidor".  **Nota:** No olvide estar posicionado sobre el nombre del servidor y no sobre un determinado sitio o carpeta virtual. Se recomienda el uso de certificados EV en la categoría alta del ENS / Difusión Limitada.
14. Comprobación de la depuración de sistemas en producción.		Compruebe que la depuración en sistemas de producción esta deshabilitada. Para ello chequee: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS) → [nombre_del_servidor] → Sitios → Editor de configuración → Sección: System.web → Compilation → Debug →False"**. 
15. Comprobación de las identidades del grupo de aplicaciones.		Compruebe que en las identidades del grupo de aplicaciones no hay identidades de servicio integradas. Para ello chequee: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS) → [nombre_del_servidor] → Grupo de aplicaciones"**. 

Comprobación	OK/NOK	Cómo hacerlo
16. Comprobación del filtrado de solicitudes.		Compruebe que está habilitado el filtrado de solicitudes. Para ello chequee: "**Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS) → [nombre_del_servidor] → Filtrado de solicitudes**". 
17. Compruebe que se encuentran deshabilitados los algoritmos SSL2, SSL3 y TLS 1.0.		Compruebe que el uso de los algoritmos SSL2, SSL3 y TLS 1.0 esté deshabilitados. Utilizando el Explorador de Windows: **"Windows+R → Regedit.exe"** Y a continuación diríjase a: "**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols"** Compruebe que existen las carpetas con los 3 algoritmos y que contienen las carpetas "Client" y "Server". Compruebe el contenido de la carpeta "Client" tal y como se muestra a continuación.  Compruebe el contenido de la carpeta "Server" tal y como se muestra a continuación. 

ANEXO A.4.3. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 INDEPENDIENTES SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tenga que securizar IIS 10 sobre Microsoft Windows Server 2016 independientes con una categorización de seguridad alta según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para los servicios e información manejada por la organización correspondieran, al menos, a la categoría alta para alguno de ellos, deberá realizar las implementaciones según se referencian en el presente anexo.

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

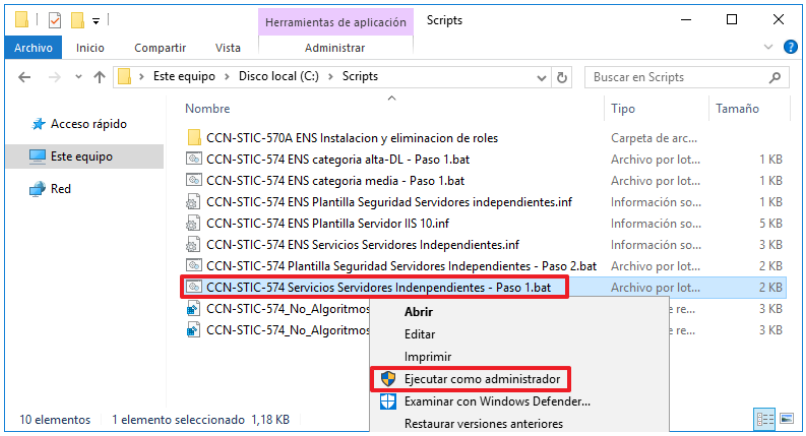
Nota: Tenga en cuenta que en el caso de una red clasificada con grado de clasificación Difusión Limitada se hará usó de la aplicación de seguridad descrita en este anexo, pero deberá atender adicionalmente a los requisitos establecidos por la normativa de aplicación sobre sistemas clasificados para dicho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

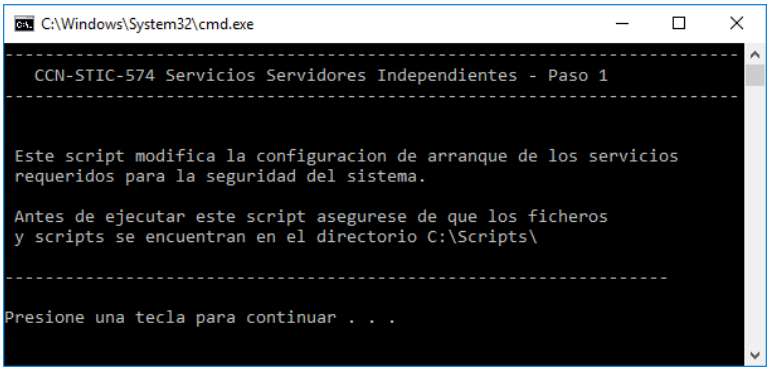
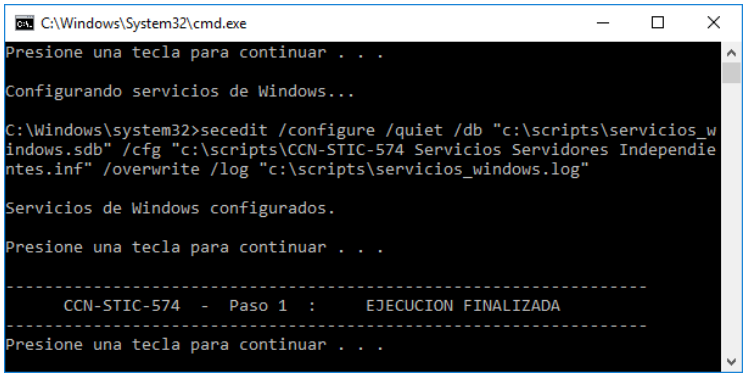
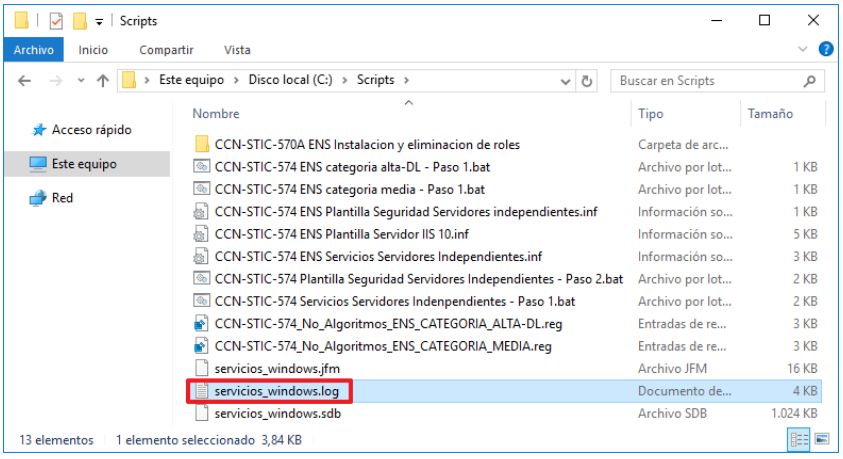
Debe tener en consideración que, antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad para comprobar su correcta funcionalidad.

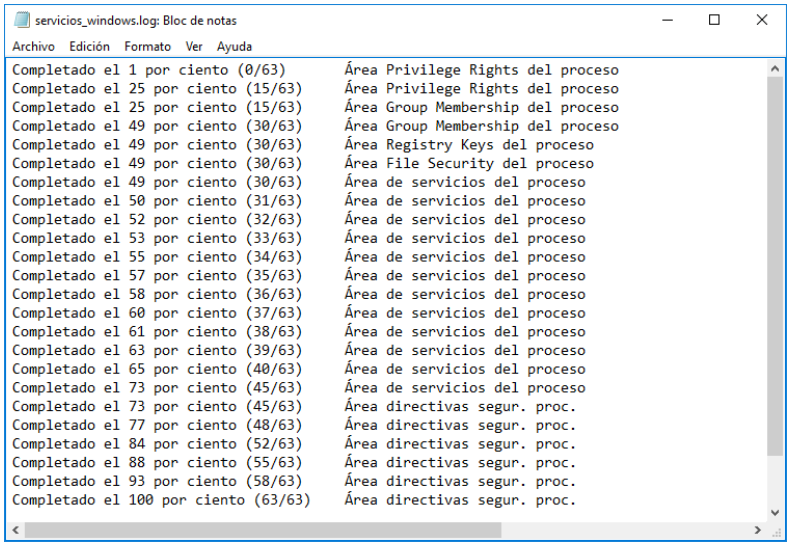
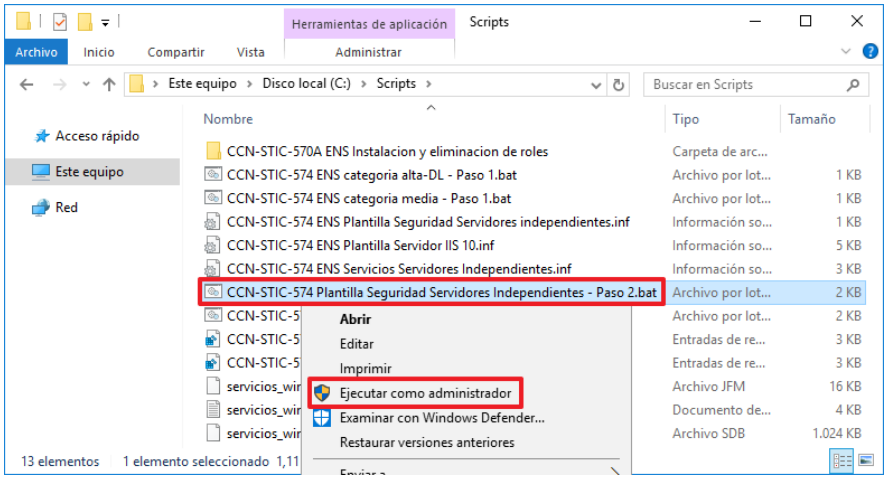
Nota: Si instala Internet Information Services por primera vez con la guía 570A o 570B aplicada debe habilitar la instalación remota de roles, características y servicios de rol a través de Shell la cual se encuentra deshabilitada por LGPO.
Si ha instalado el rol de IIS después de haber aplicado el procedimiento descrito en las guías mencionadas anteriormente, deberá volver a aplicar dicho paso a paso antes de continuar con la presente guía. Esto es debido a que durante la instalación del rol se modifican los permisos de usuario del sistema y altera el nivel mínimo de seguridad establecido por el ENS.

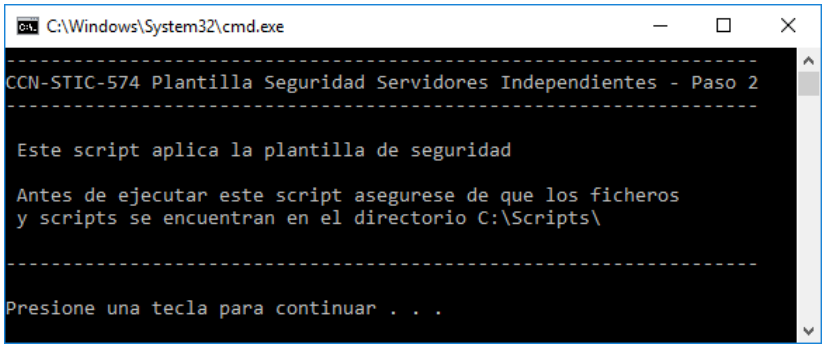
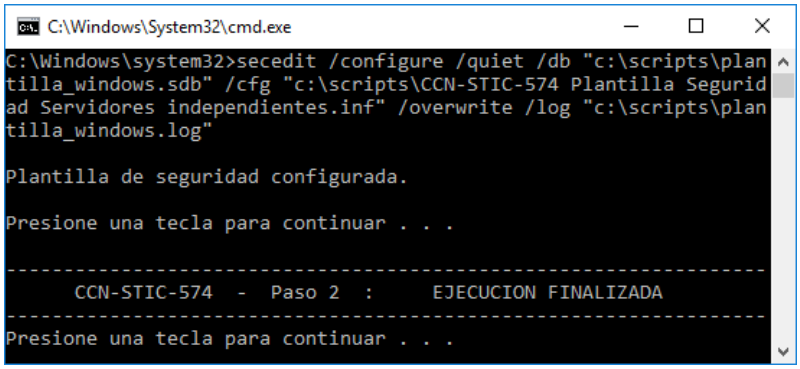
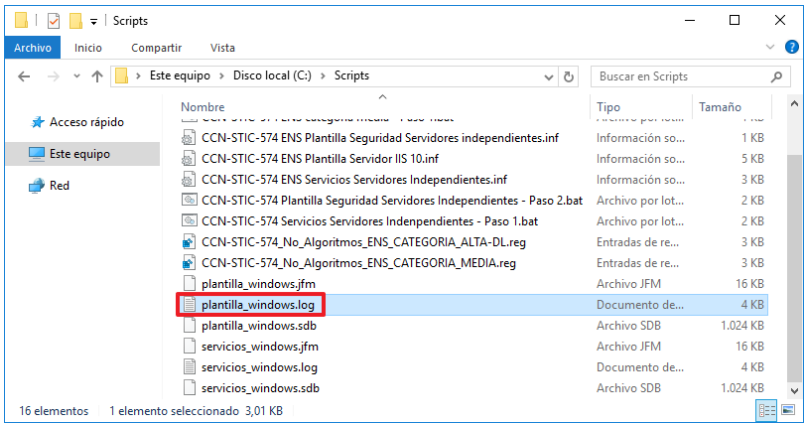
1. CONFIGURACIÓN DE LA SEGURIDAD LOCAL

Los pasos que se describen a continuación se realizarán en todos aquellos servidores IIS 10 sobre Microsoft Windows Server 2016, independientes, que implementen servicios o información de categoría alta y que se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

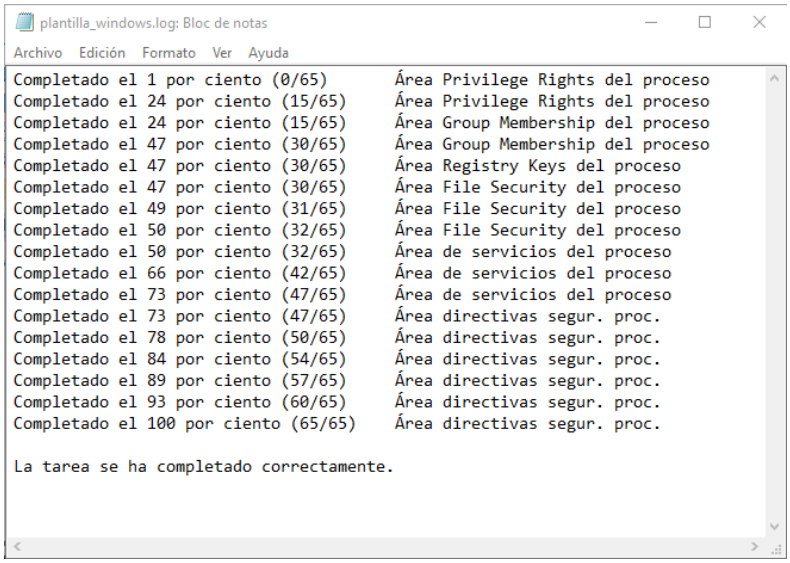
Paso	Descripción
1.	Inicie sesión en el servidor independiente donde se va aplicar seguridad según criterios de ENS. 
2.	Debe iniciar sesión con una cuenta que sea administrador del servidor.
3.	Cree el directorio “Scripts” en la unidad “C:\”.
4.	Copie los scripts asociados a esta guía en el directorio “C:\Scripts”.
5.	Abra la carpeta “C:\Scripts" y pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-574 Servicios Servidores Independientes – Paso 1.bat” y seleccione la opción “Ejecutar como administrador”.  **Nota:** En función del usuario con el que se haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que se le solicite la elevación de privilegios. Para ello introduzca las credenciales de un usuario con permisos de administrador o bien eleve automáticamente los privilegios sin necesidad de introducir usuario y contraseña.

Paso	Descripción
6.	Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la categoría alta del ENS / Difusión Limitada. 
7.	Una vez completado el proceso, deberá pulsar una tecla para continuar. 
8.	Pulse de nuevo otra tecla, para finalizar la ejecución del script. La ejecución del script genera un registro en la carpeta “C:\Scripts” con el nombre de “servicios_windows.log”. 

Paso	Descripción
9.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación. 
10.	A continuación, pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-574 Plantilla Seguridad Servidores Independientes - Paso 2.bat” y seleccione la opción “Ejecutar como administrador”.  **Nota:** En función del usuario con el que se haya validado y la configuración UAC existente antes de realizar la implementación de la presente guía, puede que se le solicite la elevación de privilegios. Para ello introduzca las credenciales de un usuario con permisos de administrador o bien eleve automáticamente los privilegios sin necesidad de introducir usuario y contraseña.

Paso	Descripción
11.	Pulse una tecla para iniciar la ejecución del script que configurará la plantilla de seguridad con la seguridad requerida para la categoría alta del ENS / Difusión Limitada. 
12.	Una vez completado el proceso, deberá pulsar una tecla para continuar. 
13.	Pulse de nuevo otra tecla, para finalizar la ejecución del script. La ejecución del script genera un registro en la carpeta “C:\Scripts” con el nombre de “plantilla_windows.log”. 

Paso	Descripción
14.	Abra este registro para comprobar si la configuración de la plantilla ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.



2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

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

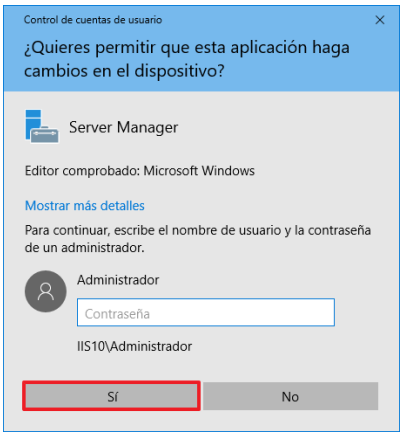
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

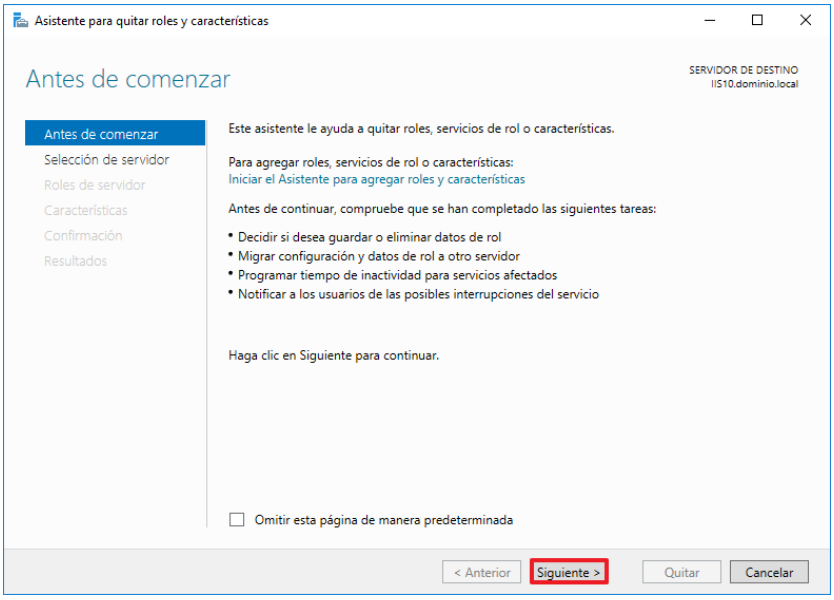
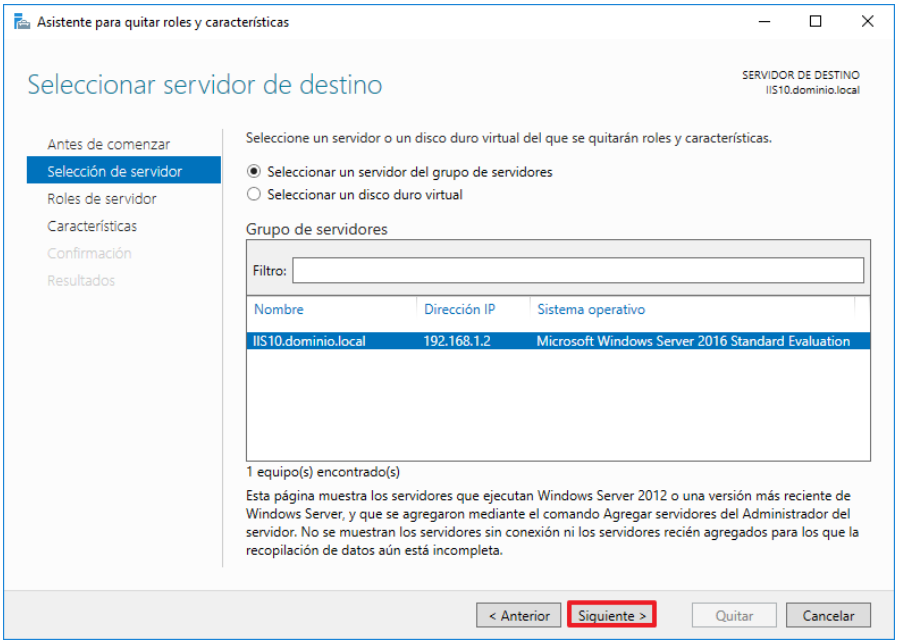
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

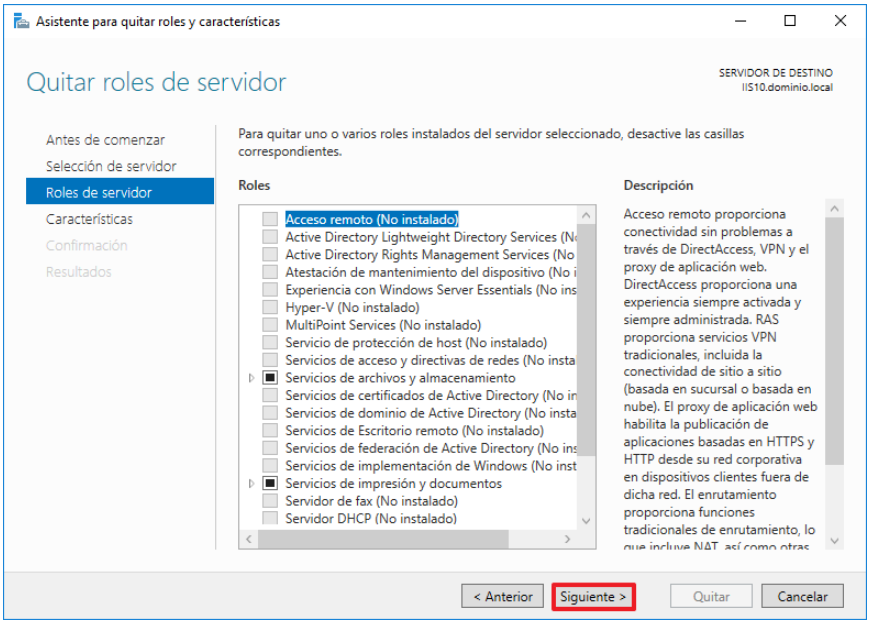
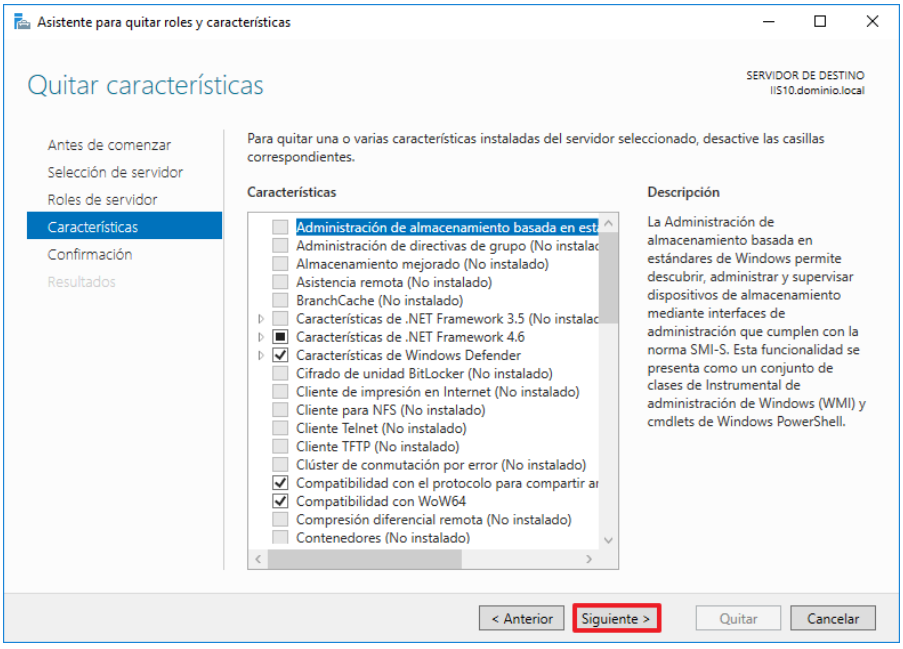
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

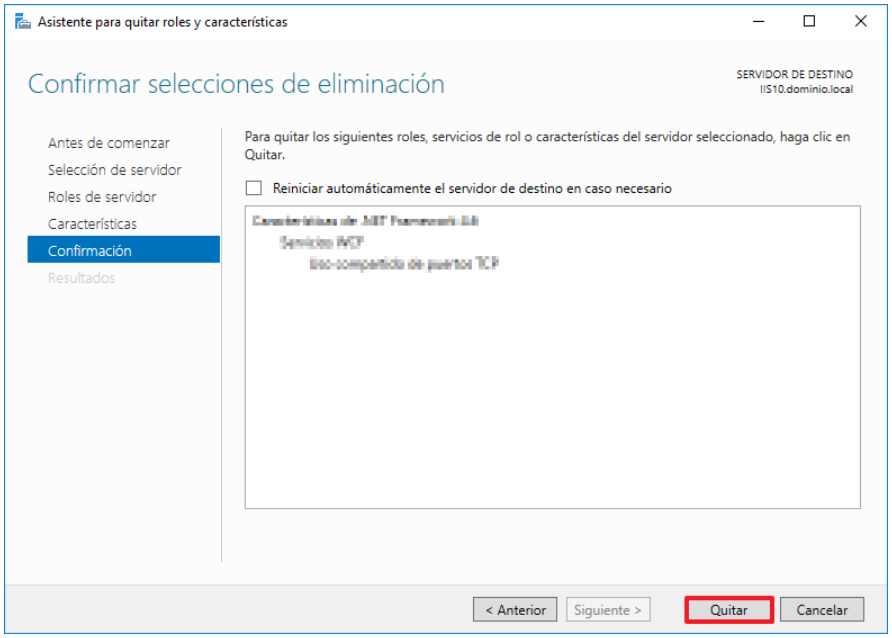
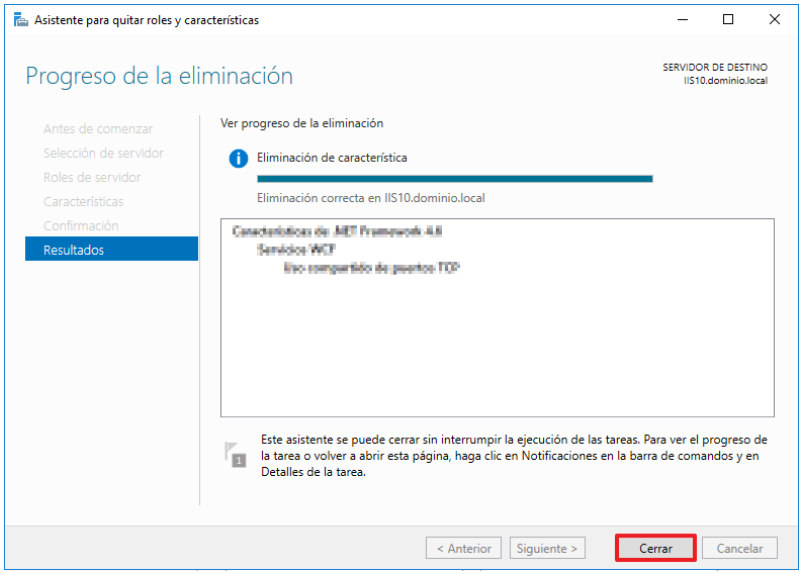
Es recomendable que el sitio web este alojado en otra ubicación de disco diferente a la del sistema operativo y que esta solo se utilice para el alojamiento de sitios web, evitando con ello exponer más información de la estrictamente necesaria.

Para realizar el siguiente paso a paso deberá realizar previamente el paso "3.1 PREPARACIÓN DEL SERVIDOR INDEPENDIENTE" y una vez finalizado deberá realizar el paso "3.4 DESHABILITACIÓN DE UNA DIRECTIVA DE GRUPO LOCAL".

Paso	Descripción
15.	A continuación, deberá iniciar sesión en el servidor independiente donde está instalado el rol de IIS 10. 
16.	Pulse sobre el administrador del servidor. 
17.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración. 
18.	A continuación, pulse sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Administrar → Quitar roles y funciones"**. 

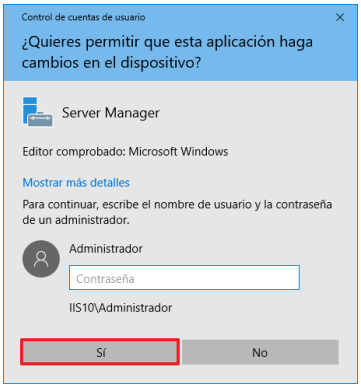
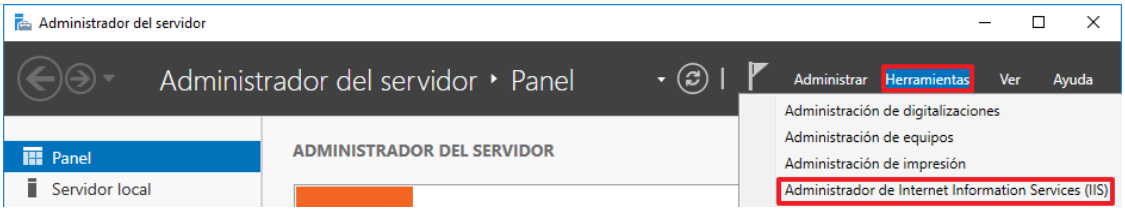
Paso	Descripción
19.	Comenzará el asistente para quitar roles y características, pulse sobre el botón “Siguiente >”. 
20.	Seleccione el servidor donde desea quitar las características del IIS 10 y pulse siguiente. 

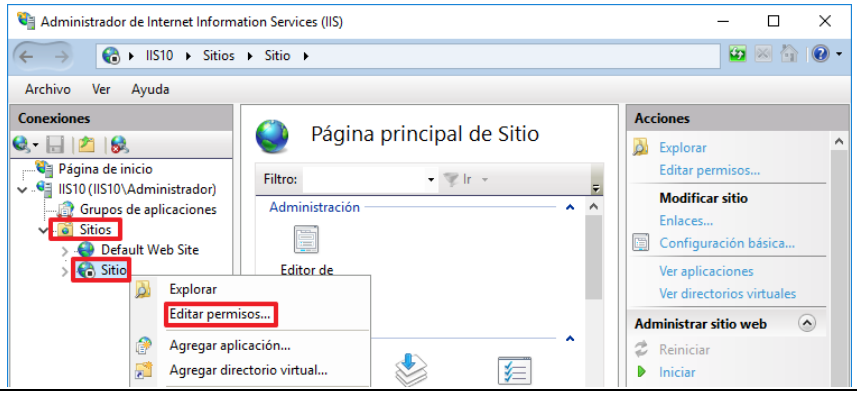
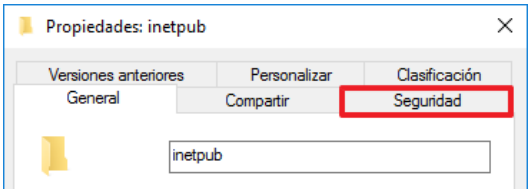
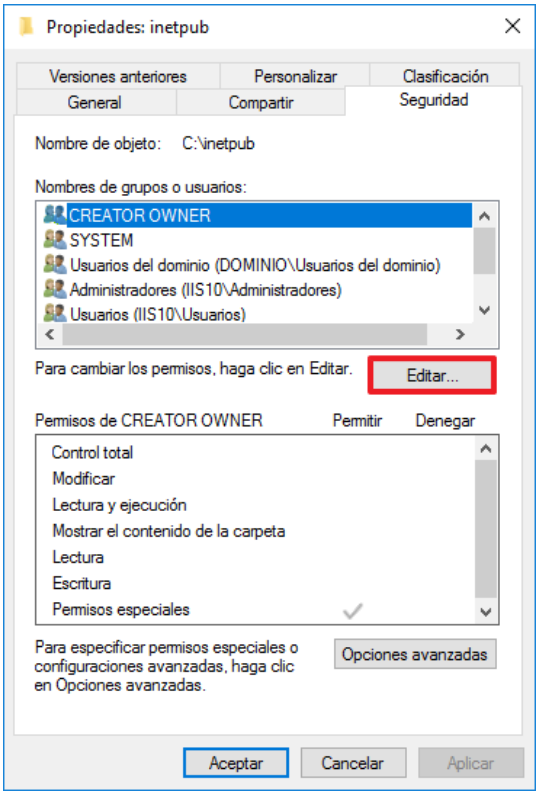
Paso	Descripción
21.	En la siguiente ventana podrá quitar roles del servidor, en este caso pulse siguiente para acceder a las características de los roles instalados. 
22.	A continuación, seleccione las características que desea quitar. 

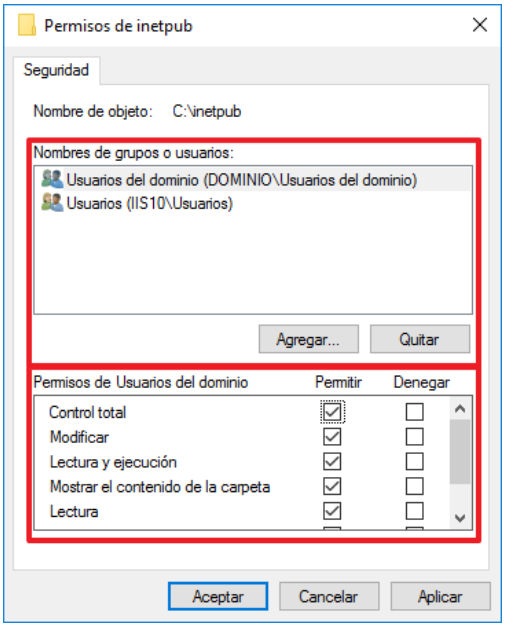
Paso	Descripción
23.	La siguiente pantalla mostrara las características a modos resumen que desea quitar, confirme que las características seleccionadas son las correctas y pulse “Quitar”. 
24.	Una vez finalizada la desinstalación pulse “Cerrar”.  **Nota:** Debe tener en cuenta que la desinstalación de determinadas características puede requerir el reinicio del equipo.

2.2. GESTIÓN DE PERMISOS RECURSOS WEB

En este apartado se tendrá en consideración la gestión y administración del acceso a los recursos web según el marco operacional de categoría alta establecido por el ENS, para con ello limitar y controlar el acceso a directorios con información sensible de ser sustraída.

Paso	Descripción
25.	Inicie sesión en el servidor independiente donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
26.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administrador. 
27.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione: **“Herramientas → Administrador de Internet Information Services (IIS)”**. 

Paso	Descripción
28.	Pulse botón derecho sobre el sitio al cual quiere asignar o quitar permisos. 
29.	Diríjase hasta la pestaña seguridad. 
30.	A continuación, pulse el botón “Editar”. 

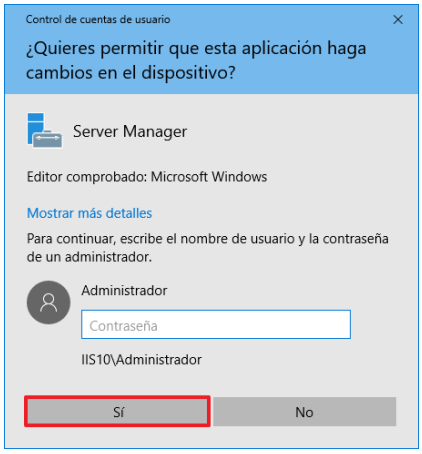
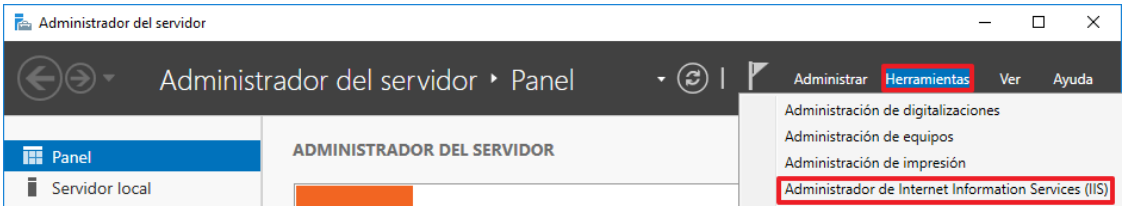
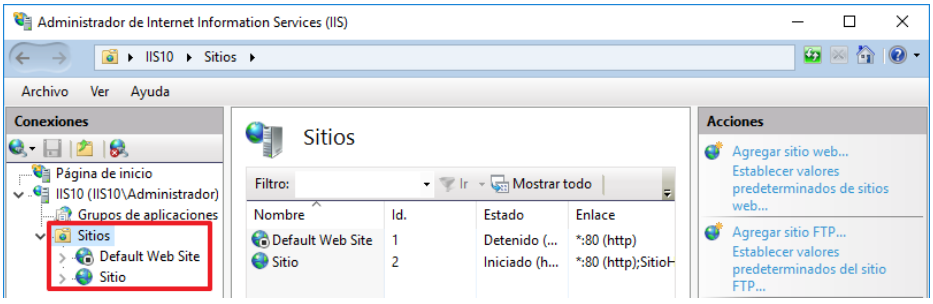
Paso	Descripción
31.	A continuación, seleccione los permisos del que desea establecer para ese sitio web.  **Nota:** Es recomendable dar permiso solo a los usuarios o grupos que deban tener acceso al sitio web evitando que el usuario administrador tenga permiso para prevenir posibles vulnerabilidades.

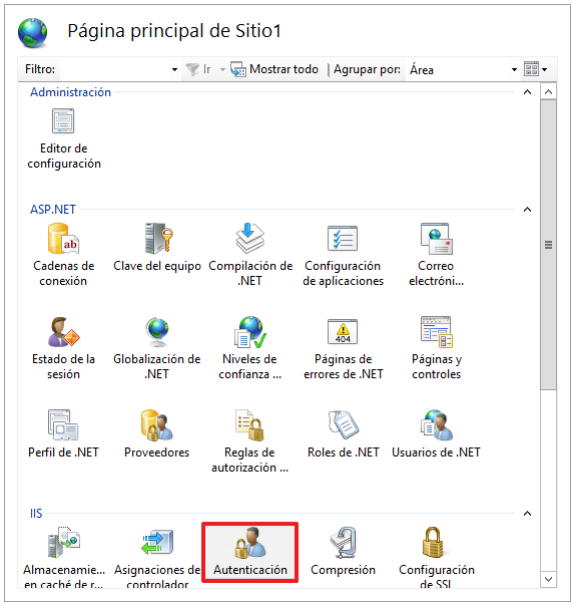
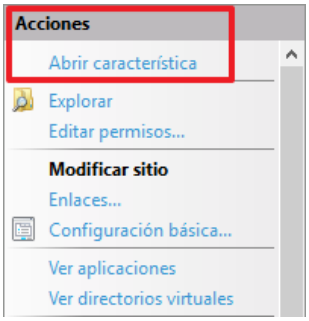
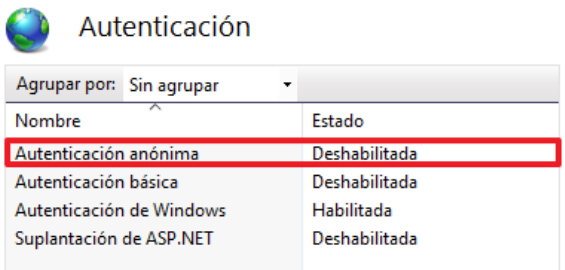
2.3. AUTENTICACIÓN SITIO WEB

Los métodos de autenticación permiten limitar el acceso al sitio web a una lista determinada de usuarios (el método habilitado por defecto de los servicios web de IIS es la autenticación anónima), en la categoría alta de categorización del ENS se recomienda habilitar los mecanismos de autenticación basados en el uso de certificados biométricos o certificados emitidos por terceros.

Los siguientes pasos indican cómo deshabilitar la autenticación anónima a nivel de sitio Web.

Paso	Descripción
32.	Inicie sesión en el servidor miembro donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 

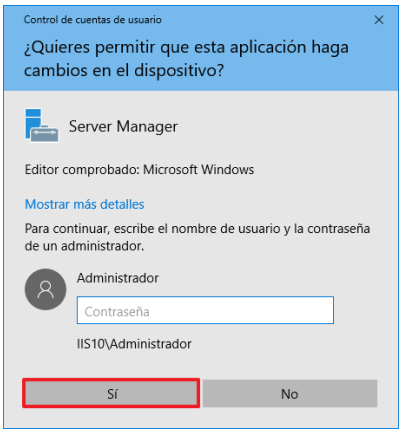
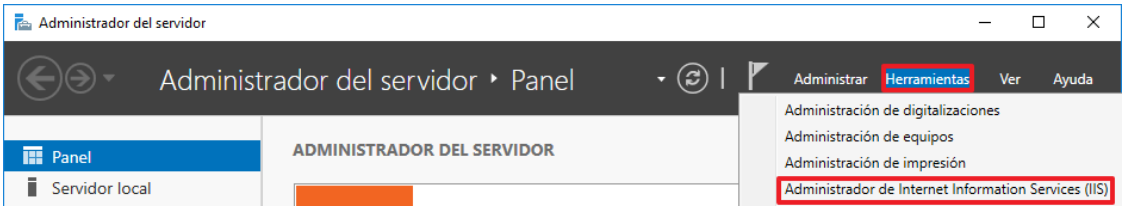
Paso	Descripción
33.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración. 
34.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione: **“Herramientas → Administrador de Internet Information Services (IIS)”** 
35.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo de “Conexiones” y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.

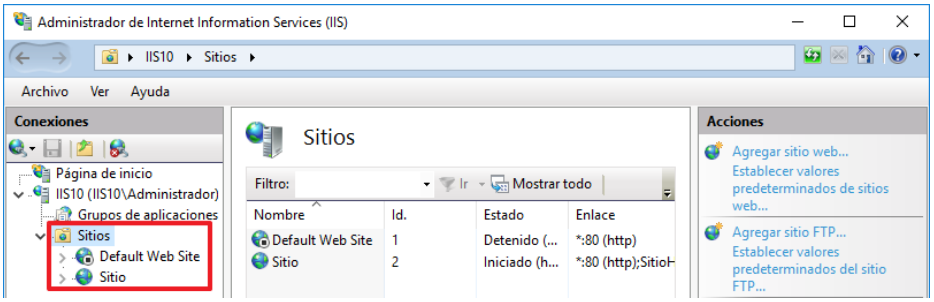
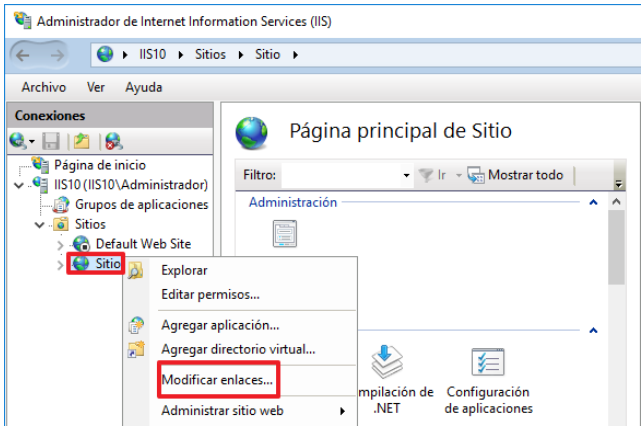
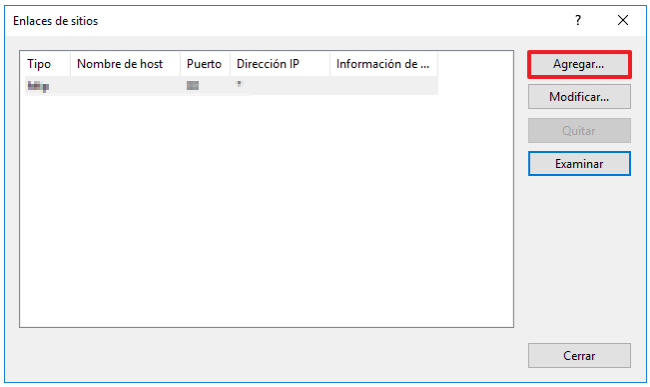
Paso	Descripción
36.	Seleccione en la página principal del sitio web el icono de “Autenticación”. 
37.	Pulse sobre “Abrir característica” situado en el panel derecho en el menú “Acciones”. 
38.	A continuación, establezca según las características de su organización los métodos de autenticación disponibles. Para ello pulse sobre el método de autenticación que quiere configurar y en el panel derecho seleccione la acción que desea realizar.  **Nota:** Únicamente se usará la autenticación anónima para páginas webs generales en la que sólo se muestre contenido y no sea necesaria la autenticación del usuario.

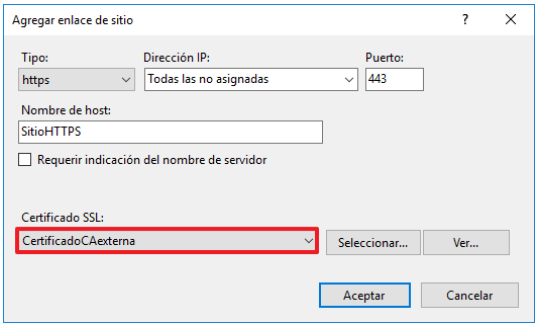
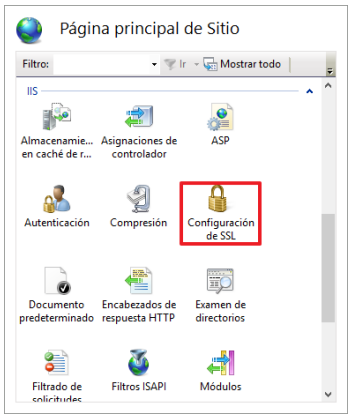
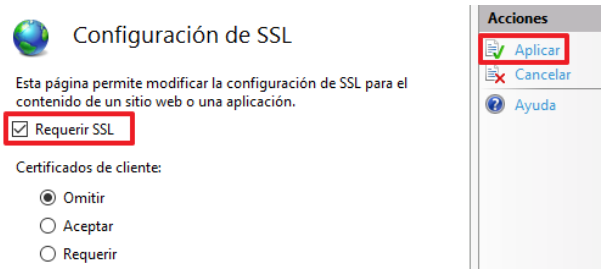
2.4. CERTIFICADOS

IIS 10 faculta el empleo de protocolos seguros para las comunicaciones y los procesos de autenticación usando HTTPS que utiliza un cifrado basado en SSL/TLS para crear un canal cifrado para el tráfico de información sensible. Para lugares públicos es un requisito indispensable en la categoría media y alta de seguridad del ENS el uso de certificados emitidos por entidades certificadoras de terceros, para el caso de sitios internos se recomienda el uso de certificados emitidos por una entidad certificadora interna, está totalmente desaconsejado el uso de certificados autofirmados.

Para la categoría más alta de seguridad del ENS es aconsejable el uso de certificados biométricos los cuales se basan en la medición de una característica física inmutable de una persona para identificar a esa persona de forma única. Las huellas digitales son una de las características biométricas más comunes.

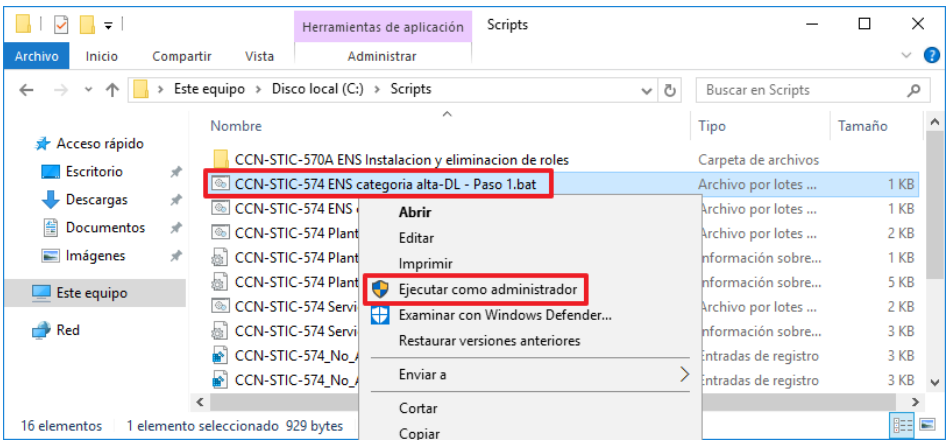
Paso	Descripción
39.	Inicie sesión en el servidor independiente donde está instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
40.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración. 
41.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”**. 

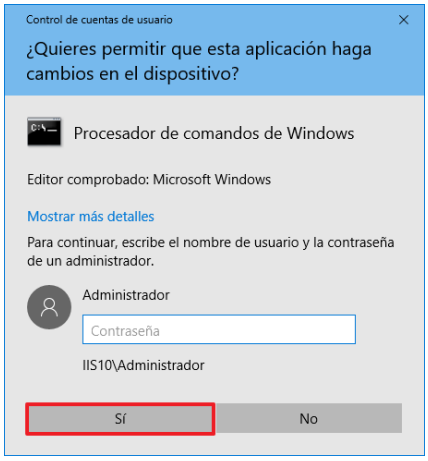
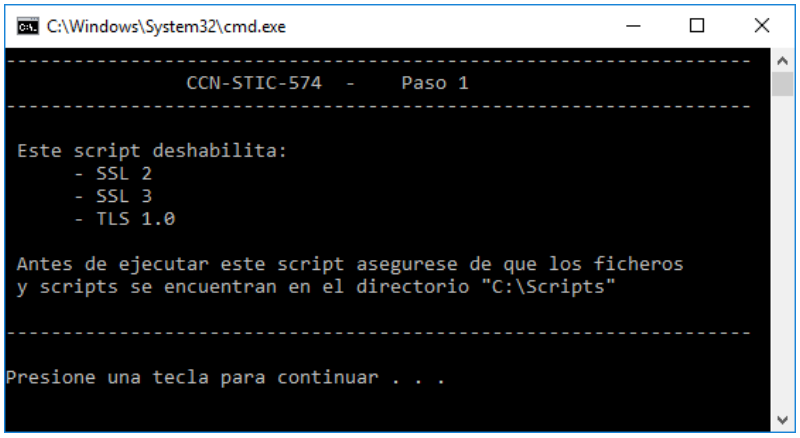
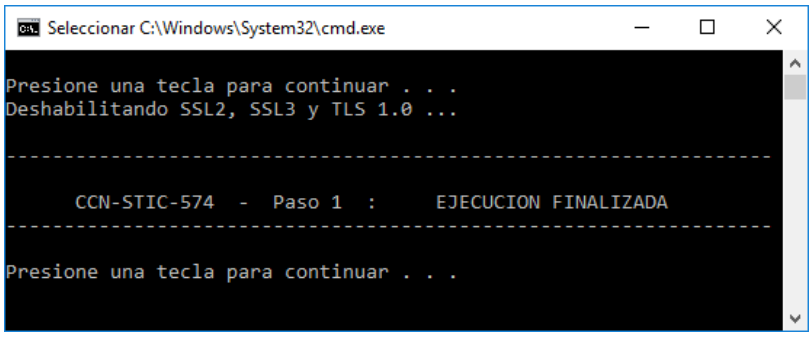
Paso	Descripción
42.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo de “Conexiones” y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.
43.	Pulse con el botón derecho sobre el sitio web que quiere modificar y seleccione la opción “Modificar enlaces…”. 
44.	Pulse sobre el botón “Agregar…”. 

Paso	Descripción
45.	Seleccione Tipo: “https”, seleccione Certificado SSL: “CertificadoCAExterna” y pulse “Aceptar”.  **Nota:** El certificado “CertificadoCAexterna” es uno ficticio creado para este ejemplo, deberá usar el adecuado para su organización.
46.	A continuación, deberá configurar el sitio web para que los usuarios requieran un certificado propio, para ello pulse sobre en el sitio web que desea configurar, y seleccione “Configuración de SSL”. 
47.	Seleccione la opción de “Requerir SSL” y pulse sobre “Aplicar” para que el sistema guarde los cambios realizados. 
48.	En caso de que usted no cuente con un certificado emitido por una entidad certificadora autorizada debe solicitarlo para cumplir con la categoría alta de seguridad del ENS.

2.5. PROTOCOLOS DE TRANSMISIÓN

Con la aplicación del ENS para la categoría alta sobre IIS 10 es imprescindible eliminar el uso de los algoritmos SSL2, SSL3 y TLS1.0, evitando con ello sufrir posibles ataques.

Paso	Descripción
49.	Inicie sesión en el servidor independiente donde tiene instalado el rol de IIS 10. 
50.	Si no lo ha realizado anteriormente, cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
51.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.
52.	A continuación, debe ejecutar el *script* 1 para deshabilitar los protocolos anteriormente indicados, es necesario realizar esta acción con elevación de privilegios, debe hacer clic con el botón derecho, sobre el fichero denominado “CCN-STIC-574 ENS categoria alta-DL - Paso 1.bat” situado en C:\Scripts y haga clic en “Ejecutar como administrador”. 

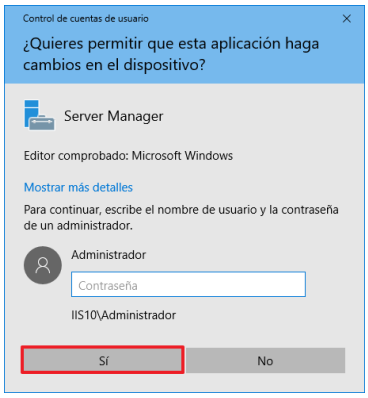
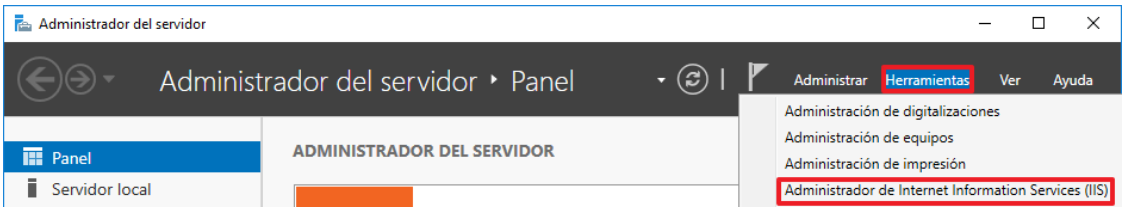
Paso	Descripción
53.	El control de cuentas de usuario le solicitará permisos para ejecutar el programa, introduzca las credenciales y pulse “Sí”. 
54.	Aparecerá la siguiente ventana, pulse cualquier tecla para continuar. 
55.	Una vez finalizada la tarea pulse una tecla para cerrar la ventana. 

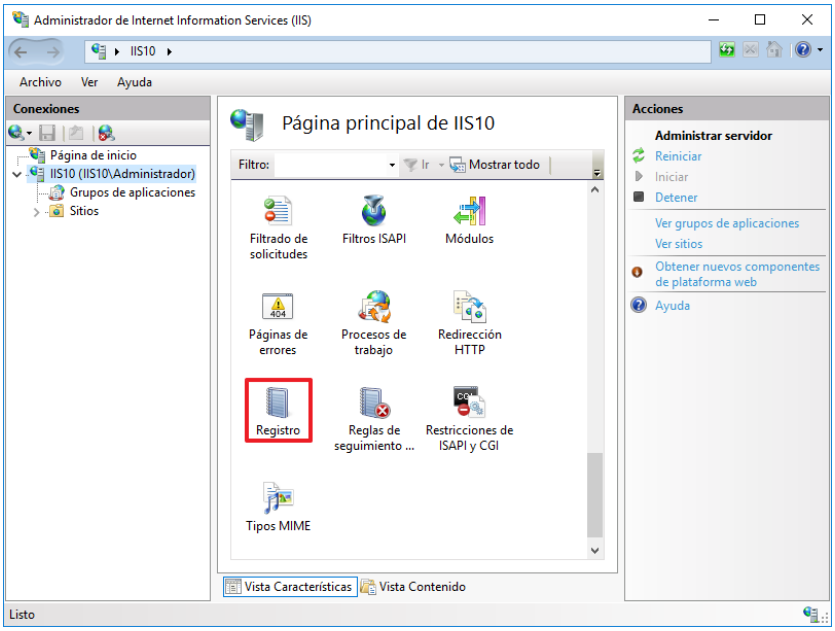
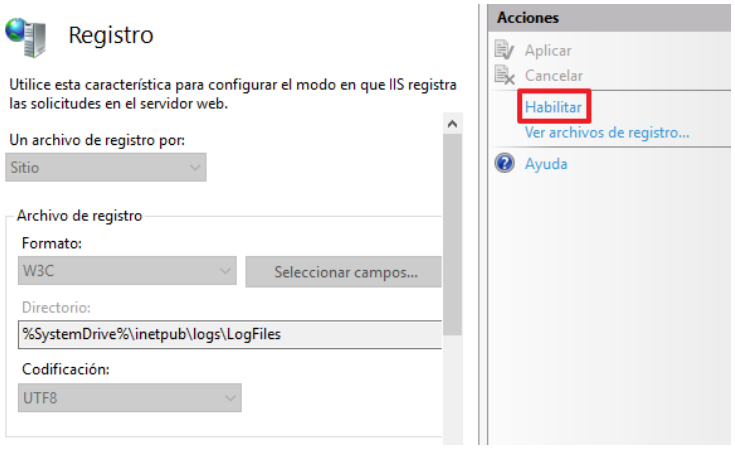
2.6. AUDITORÍA

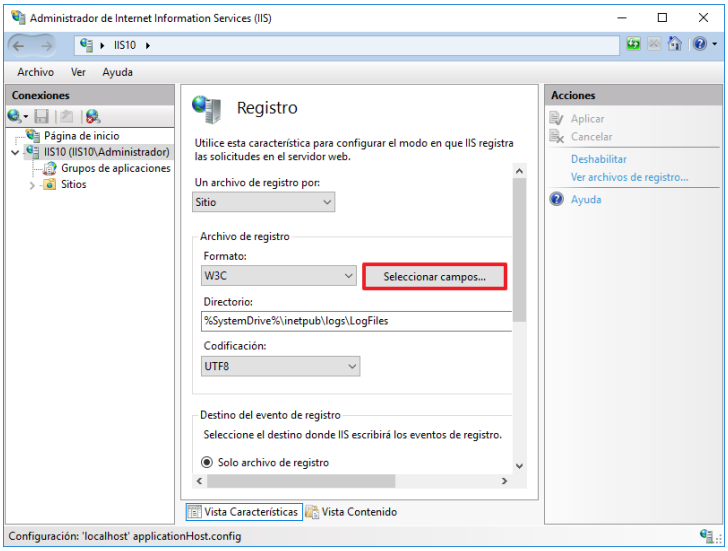
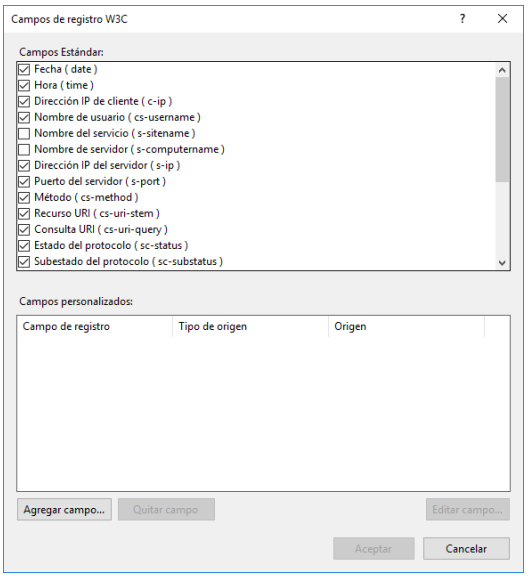
Con la aplicación del ENS para la categoría alta sobre IIS 10 quedará registrado el uso del sistema para poder detectar y reaccionar a cualquier fallo accidental o deliberado, quedando registrado en el sistema quien realiza la actividad, cuando y sobre qué información con el fin de detectar anomalías o intentos frustrados de acceso a información no autorizada.

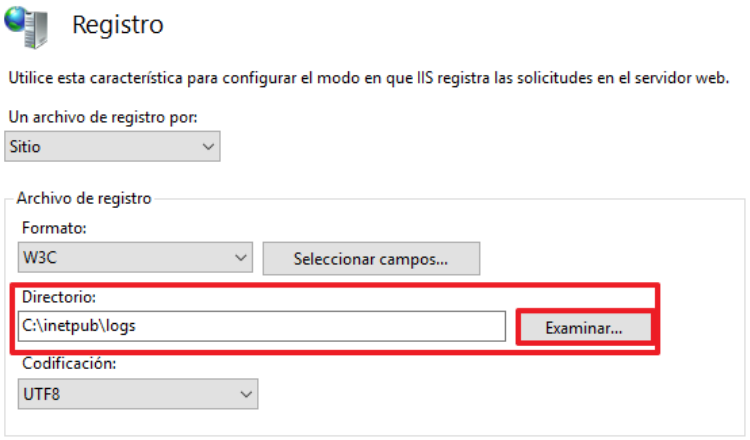
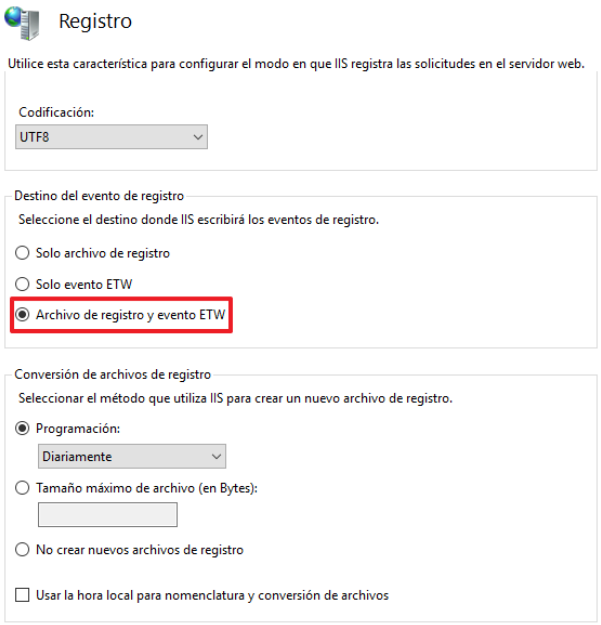
La ubicación de los registros debe ser diferente a la del sistema además de tener limitado el acceso únicamente a los usuarios autorizados.

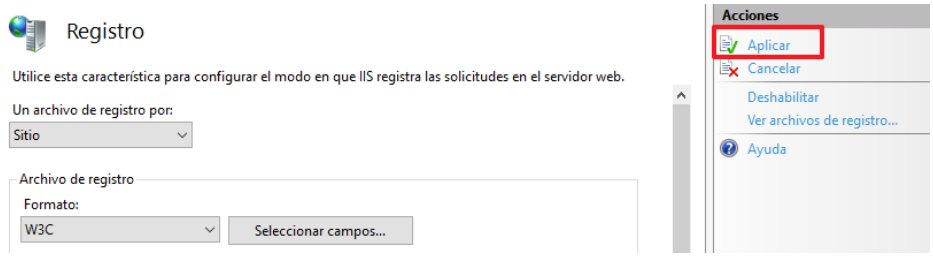
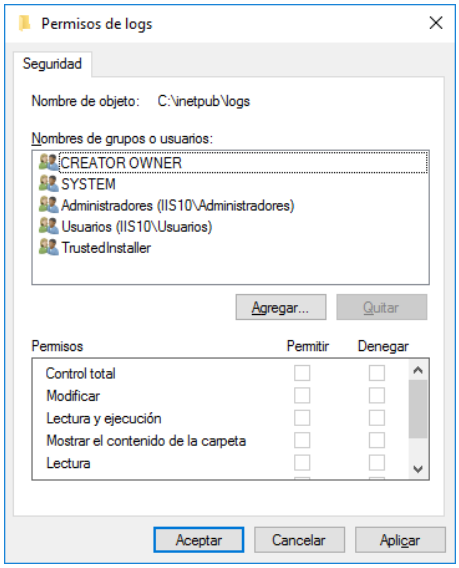
Es recomendable en la categoría alta del marco del ENS el uso de herramientas de consolidación de eventos con el fin de tener centralizada toda la información relevante obtenida de los registros en un único punto y en orden cronológico. Muchas herramientas de consolidación son capaces de elaborar alertas más elaboradas basándose en los eventos recibidos de las diversas fuentes de información.

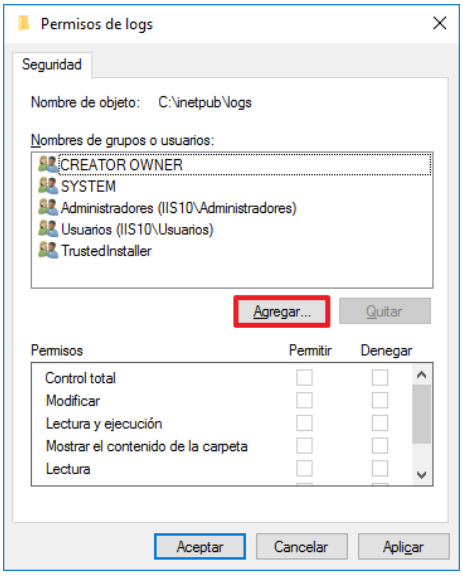
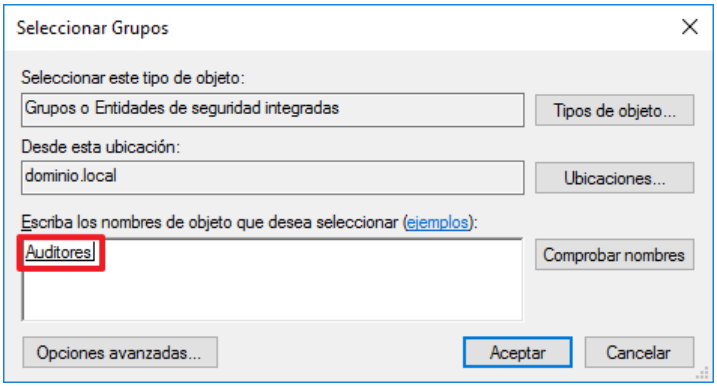
Paso	Descripción
56.	Inicie sesión en el servidor independiente donde tiene instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
57.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración. 
58.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administrador de Internet Information Services (IIS)”**.  V

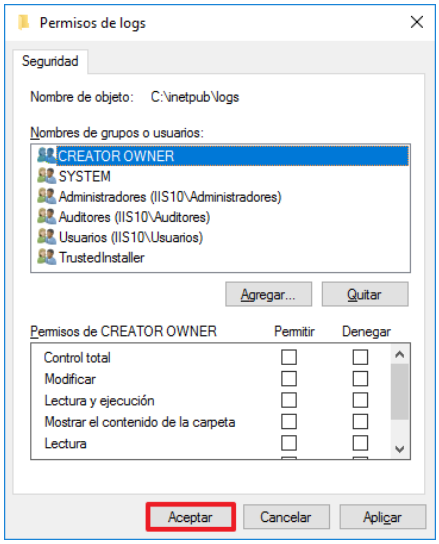
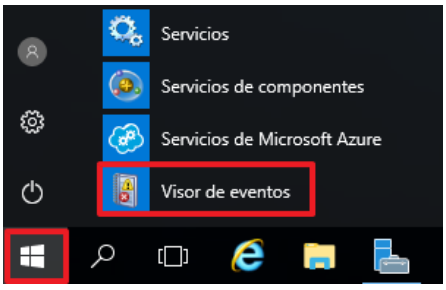
Paso	Descripción
59.	Diríjase al sitio web que desea administrar, a continuación, localice el icono “Registro”, y pulse la acción “Abrir característica” situado en la parte superior derecha de la pantalla para acceder a la configuración del registro. 
60.	Debe habilitar el registro de las solicitudes del servidor IIS 10 para ello, diríjase al menú “Acciones” situado en la parte superior derecha de la pantalla y pulse sobre “Habilitar”. 

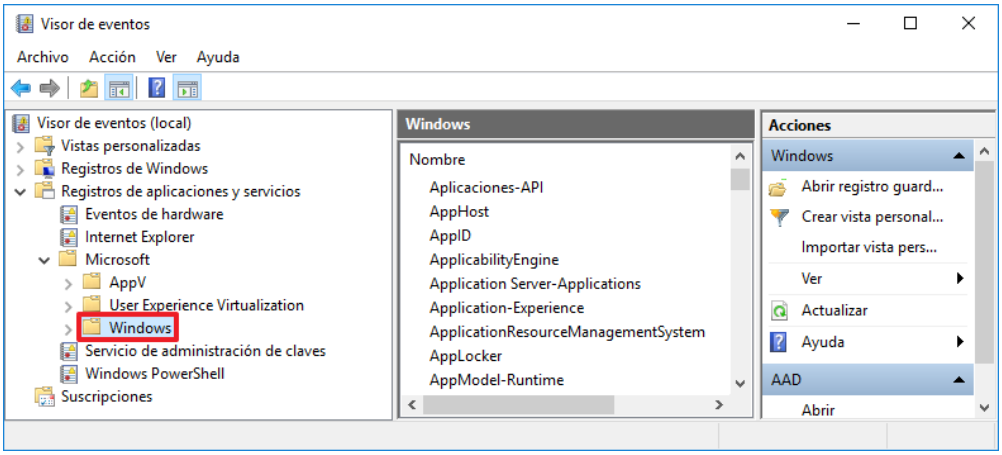
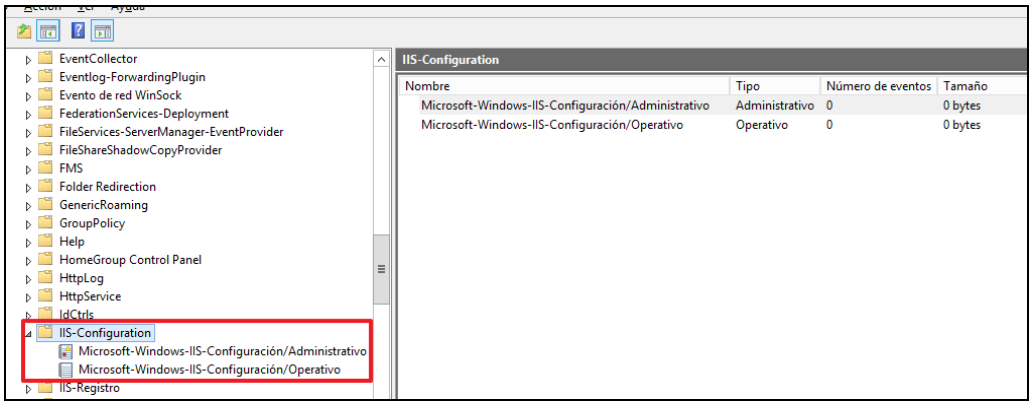
Paso	Descripción
61.	Seleccione los campos que desea registrar, para ello pulse sobre “Seleccionar campos…”. 
62.	Compruebe qué campos se recogerán en el fichero de registro y asegúrese que coincide con sus necesidades. Los valores marcados por defecto suelen ser suficientes, pero no descarte marcar otros. 

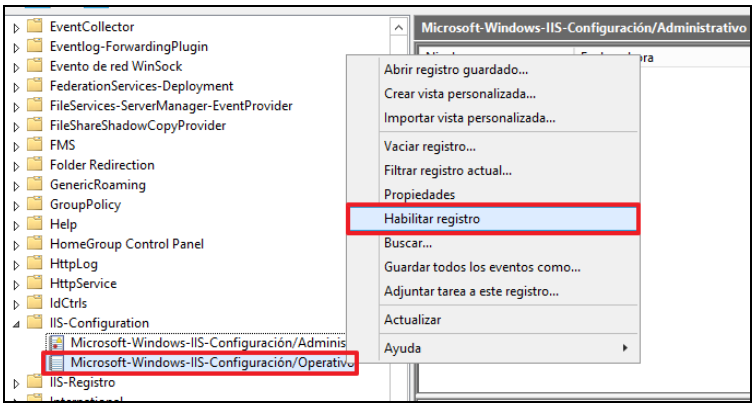
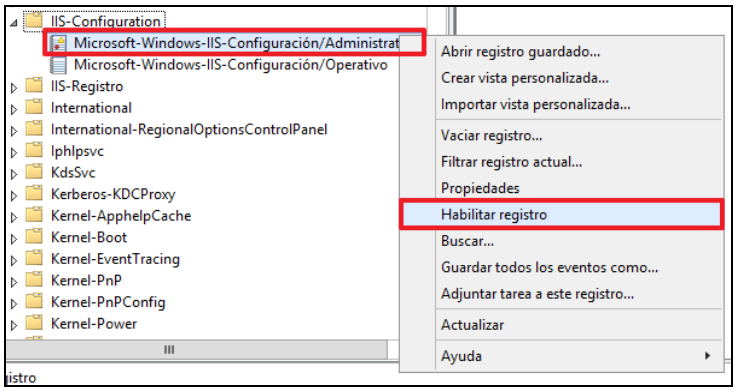
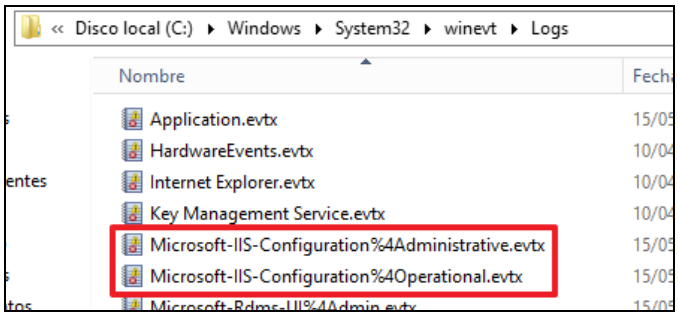
Paso	Descripción
63.	A continuación, seleccione el directorio donde se van a guardar los registros, por seguridad es recomendable realizarlo en una unidad diferente a la de la instalación del sistema operativo. 
64.	A continuación, deberá seleccionar el destino del evento, seleccione, “Archivo de registro y evento ETW”. 

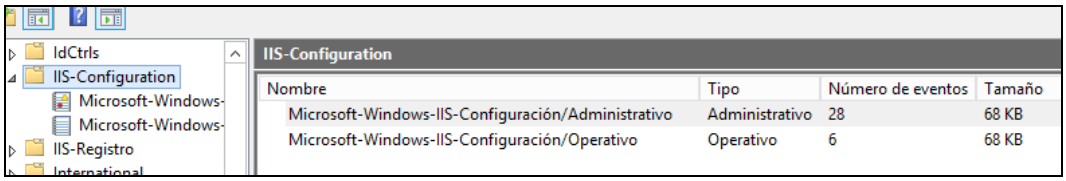
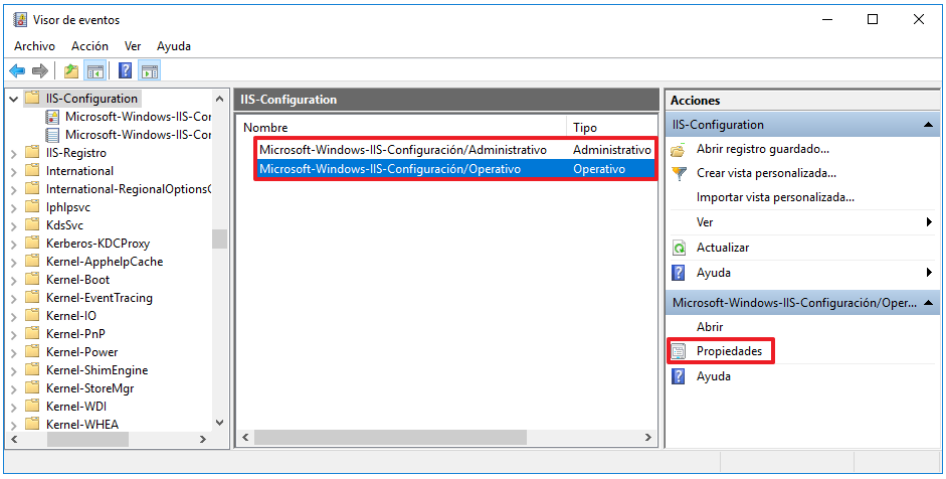
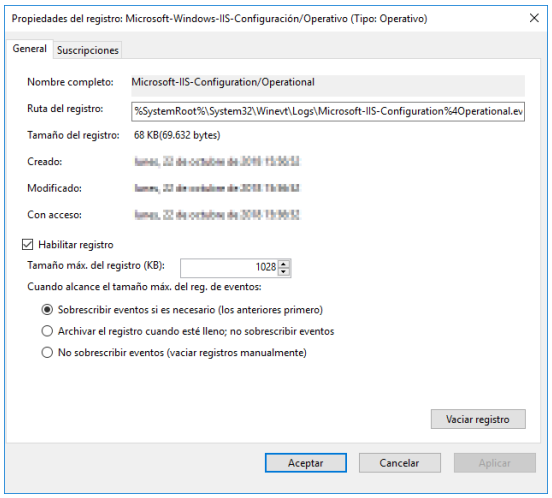
Paso	Descripción
65.	Una vez realizados los cambios deberá guardarlos, para ello pulse “Aplicar” situado en el menú “Acciones” en la parte superior izquierda de la pantalla. 
66.	A continuación, localice la carpeta **C:\INETPUB\logs**, y con el botón derecho seleccione “Propiedades”. **Nota:** Si no dispone de la carpeta “C:\INETPUB\logs” deberá crearla o adaptar los pasos a su organización.
67.	Sitúese en la pestaña “Seguridad”, donde observa que la carpeta tiene permisos aplicados directamente (los *tics* en la columna “Permitir” están en negro, no en aguadilla).  Presione “Editar” para modificar los permisos. Se detalla a continuación la actuación. **Nota:** Los permisos aplicados al usuario que ha tomado posesión de la carpeta son normales y puede ignorarlos o eliminarlos. Si el usuario no está autorizado a auditar ficheros de registro o se desea cambiar se debe hacer en la carpeta desde donde se heredan los permisos de ésta, C:\INETPUB\logs

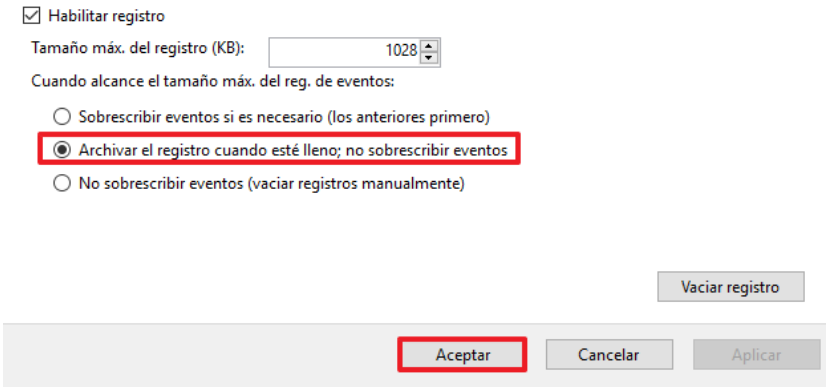
Paso	Descripción
68.	Presione el botón “Agregar…”, para en los siguientes pasos añadir al grupo Auditores.  **Nota:** Si no dispone del grupo Auditores deberá crearlo previamente para poder añadirlo.
69.	Escriba “Auditores” y acepte para que se añada. 

Paso	Descripción
70.	Los permisos que se adjudican por defecto, lectura, para los "Auditores" son los deseados por lo que puede continuar el proceso haciendo clic en el botón "Aceptar" en la ventana "Permisos de logs", y de nuevo "Aceptar" en la ventana "Propiedades: logs". 
71.	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.
72.	Debe abrir el Visor de eventos, ejecutándolo como administrador, como en ocasiones anteriores, "**Menú inicio→ Herramientas administrativas→ Visor de eventos**".  **Nota:** El sistema solicitará elevación de privilegios para completar la acción.

Paso	Descripción
73.	Seleccione en el árbol **"Visor de eventos→ Registro de aplicaciones y servicios→ Microsoft → Windows"**. 
74.	Desplácese hacia abajo, podrá observar que Microsoft Windows Server 2016 dispone de dos grupos de registros para IIS, dentro del de configuración se encuentran: administrativo y operaciones. Es necesario activar ambos, según se le indica a continuación. 

Paso	Descripción
75.	Sitúese sobre el registro operativo, abra el menú contextual con el botón derecho del ratón y seleccione “Habilitar registro”.  **Nota:** Cualquier acción operativa sobre el servidor quedará recogida a partir de ahora.
76.	Haga lo mismo para el registro “Administrativo”. 
77.	Los registros se habrán creado en el disco duro, en la partición del sistema operativo (habitualmente la C:) y en la ruta **%SystemRoot%\System32\winevt\Logs**, con los nombres: Microsoft IIS-Configuration%4Operational.evtx y Microsoft IIS-Configuration%4Administrative.evtx  **Nota:** La variable %SystemRoot% corresponde a C:\Windows\System32 en las configuraciones habituales de las guías.

Paso	Descripción
78.	Los ficheros se crean con tamaño cero pero se empezarán a poblar automáticamente desde este momento: 
79.	Para acceder a las propiedades de los ficheros, seleccione un fichero y pulse sobre la opción “Propiedades” del menú “Acciones”.  **Nota:** Tenga en cuenta que el registro administrativo se llenará, en condiciones normales, antes que el operacional.
80.	La siguiente pantalla muestra la configuración, propiedades, por defecto.  **Nota:** Tenga en cuenta que el registro administrativo se llenará, en condiciones normales, antes que el operacional.

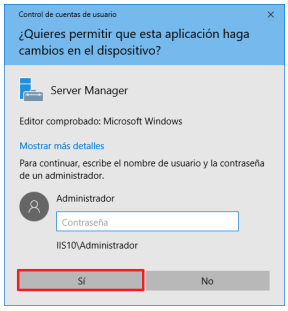
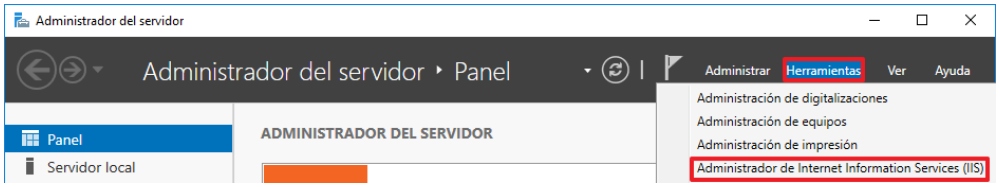
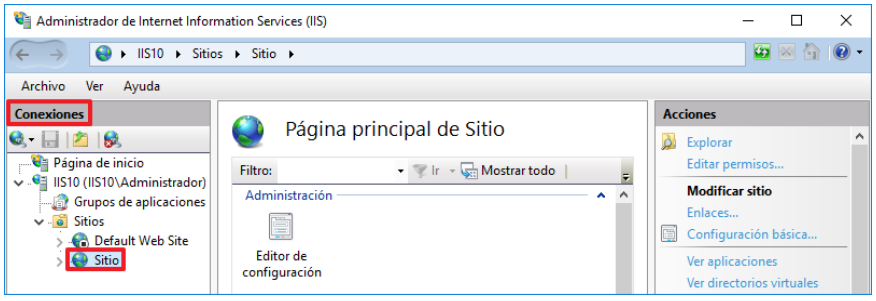
Paso	Descripción
81.	Para evitar, que una vez completado el fichero de registro, se empiece a borrar por la entrada más antigua para reutilizar espacio, y dado que en muchas ocasiones las necesidades de seguridad de una organización priman, debe marcar la opción que permite no perder registros, pero 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".
82.	Con la configuración dejada, 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". Y el fichero de auditoría se vacía y comienza a llenarse de nuevo. **Nota:** Estos ficheros deberán ser copiados y eliminados periódicamente para evitar su pérdida y el llenado del disco duro.

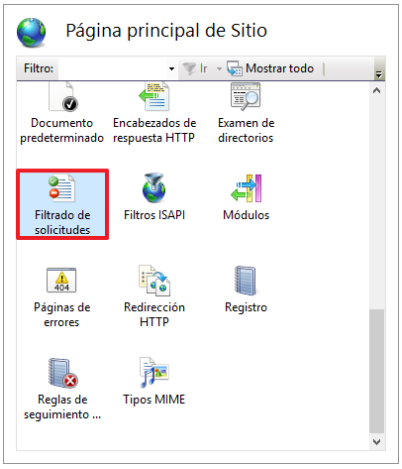
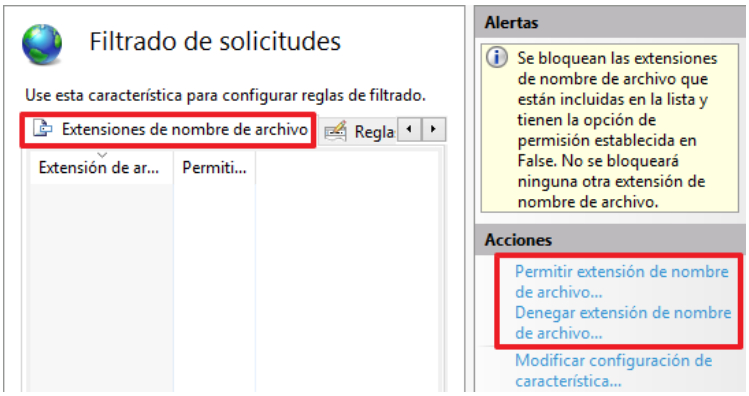
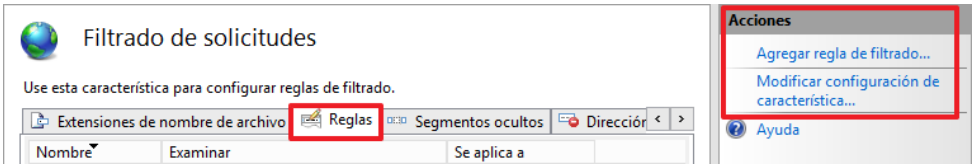
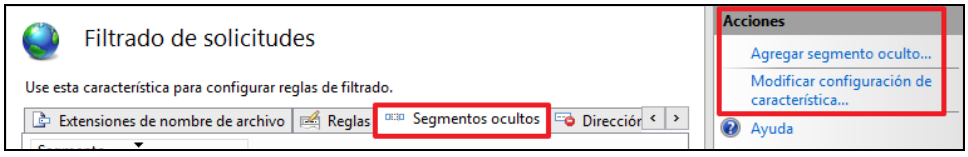
2.7. FILTRADO DE SOLICITUDES

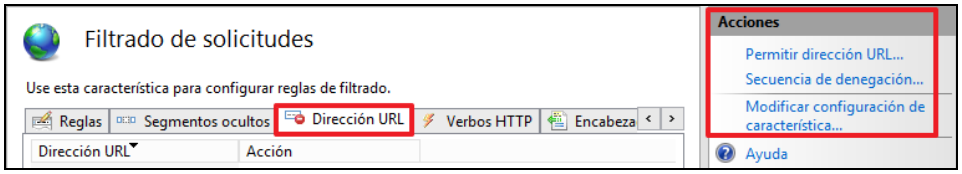
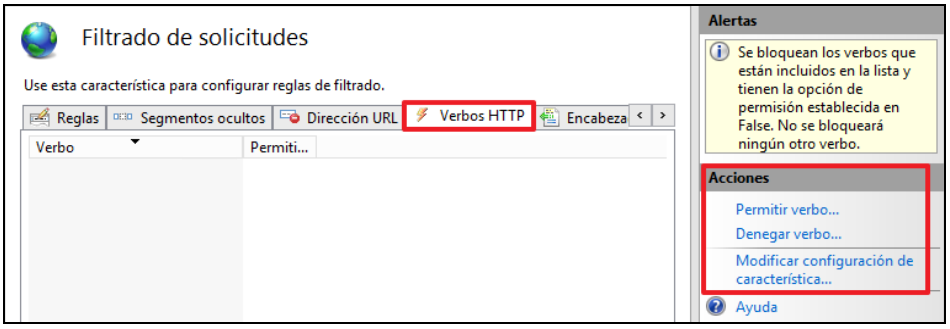
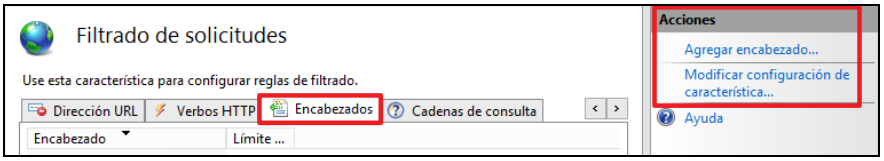
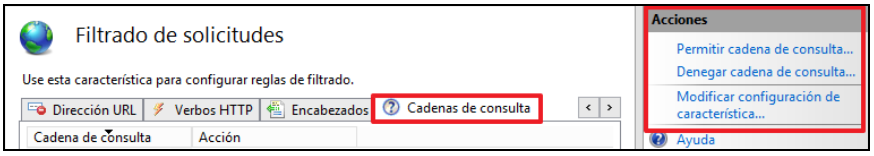
El siguiente paso define el procedimiento para la configuración del filtro de solicitudes el cual se encarga de analizar todas las solicitudes que entran en el servidor web y las filtra basándose en reglas establecidas previamente.

La mayoría de los ataques malintencionados comparten características comunes, como direcciones URL muy largas o solicitudes de una acción inusual, es por ello que filtrando las solicitudes se puede reducir el impacto de este tipo de ataques.

Cada organización debe determinar que extensiones son las específicamente necesarias para la funcionalidad del sitio web que tiene alojado y deberá configurar el filtro para soportar únicamente las extensiones exclusivamente necesarias.

Paso	Descripción
83.	Inicie sesión en el servidor independiente donde tiene instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
84.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración. 
85.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione: **“Herramientas → Administrador de Internet Information Services (IIS)”** 
86.	Una vez iniciado el Administrador de Internet Information Services (IIS), navegue por el panel izquierdo de “Conexiones” y localice el sitio web que desea configurar.  **Nota:** Los nombres usados para la realización de esta guía son ficticios, por lo que usted debe adaptar estos pasos al entorno de su organización.

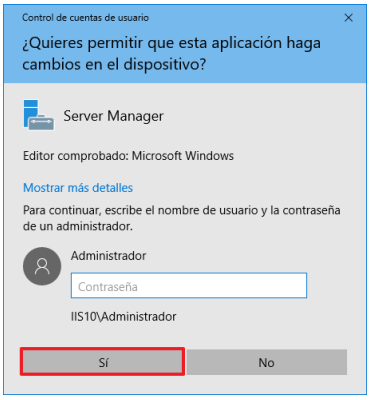
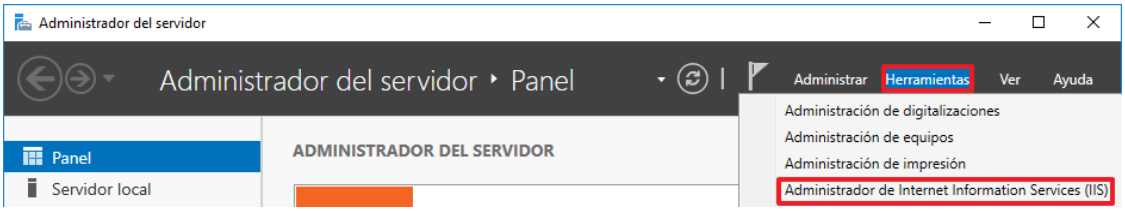
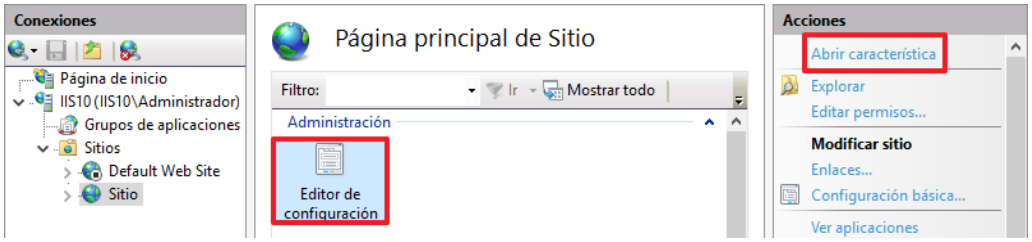
Paso	Descripción
87.	Seleccione en la página principal del sitio web el icono “Filtrado de solicitudes” y pulse sobre “Abrir característica” sitiado en el menú acciones del panel superior derecho de la pantalla. 
88.	A continuación, en la pestaña “Extensiones de nombre de archivo” puede permitir o denegar extensiones que no estén incluidas en la lista. 
89.	En la siguiente pestaña puede agregar o modificar reglas de filtrado. 
90.	En la siguiente pestaña puede agregar o modificar segmentos ocultos. 

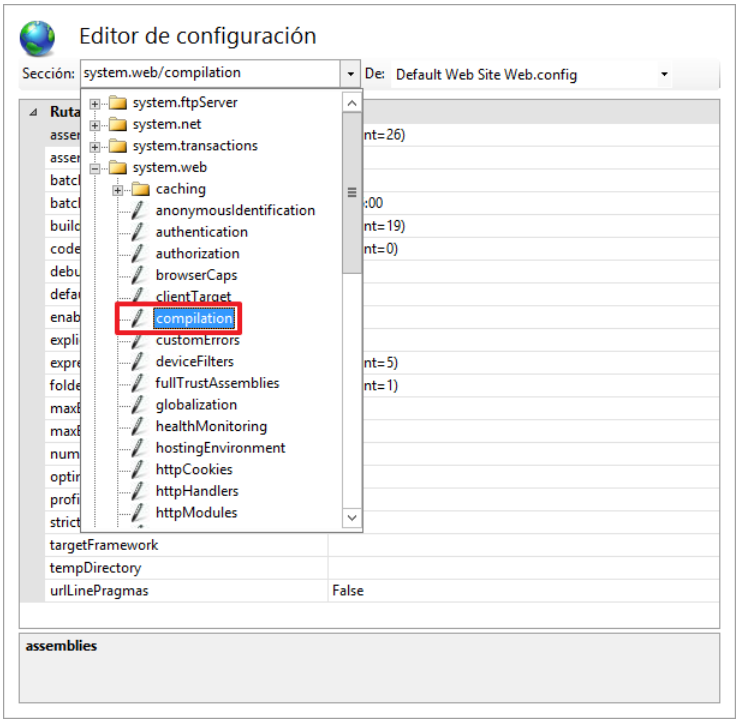
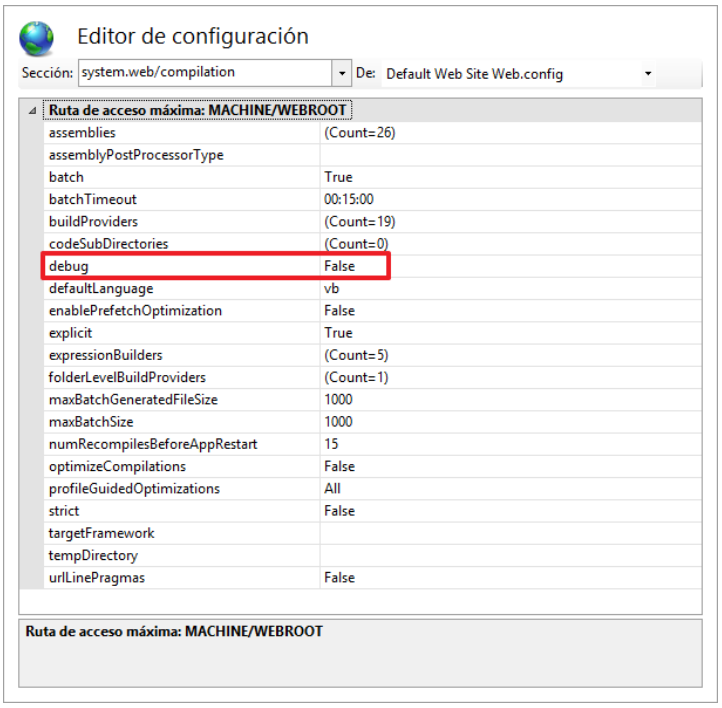
Paso	Descripción
91.	En la siguiente pestaña puede permitir, denegar o modificar direcciones URL. 
92.	En la siguiente pestaña puede permitir, denegar o modificar Verbos. 
93.	En la siguiente pestaña puede agregar o modificar encabezados. 
94.	En la siguiente pestaña puede permitir, denegar o modificar cadenas de consulta. 

2.8. DESHABILITAR MODOS DE DEPURACIÓN

El siguiente paso define el procedimiento para la modificación del fichero web.config para inhabilitar el modo de depuración de una aplicación en entornos de producción, evitando con ello posibles fisuras de seguridad.

Paso	Descripción
95.	Inicie sesión en el servidor independiente donde tiene instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 

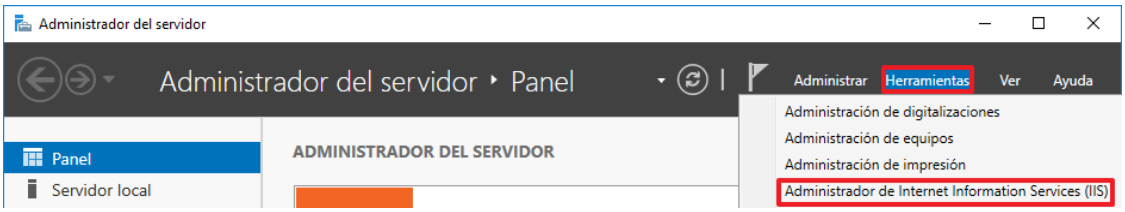
Paso	Descripción
96.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración. 
97.	Inicie la herramienta “Administrador de Internet Information Services (IIS)”. Para ello, pulse sobre el menú superior de la derecha de la herramienta “Administrador del servidor” y seleccione: **“Herramientas → Administrador de Internet Information Services (IIS)”** 
98.	Localice el sitio web que desea configurar y seleccione “Editor de configuración”, a continuación, pulse en el menú “Acciones” la opción “Abrir característica” situado en la parte superior derecha de la pantalla para abrir el editor de configuración. 

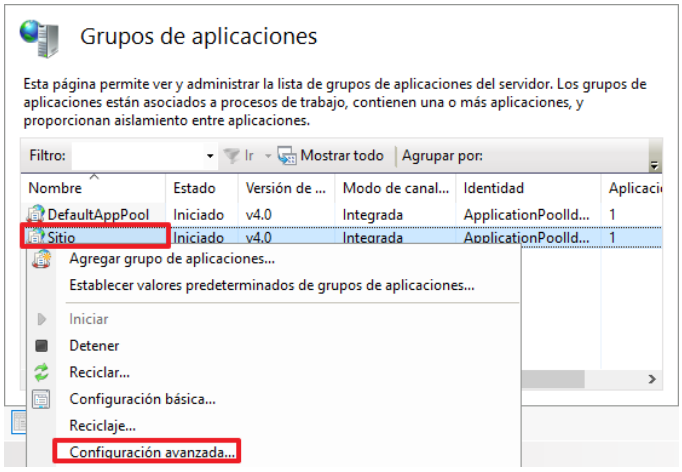
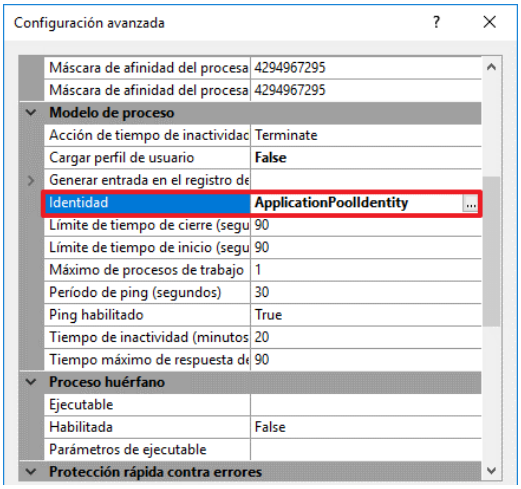
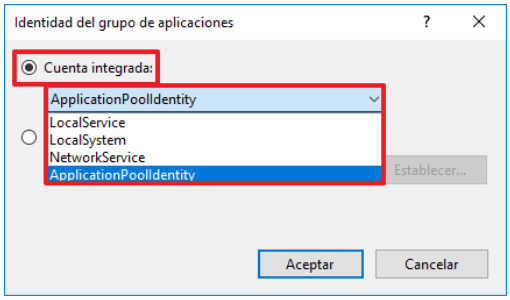
Paso	Descripción
99.	Navegue en “Sección” hasta “system.web/compilation”. 
100.	Localice la opción “Debug”, abra el desplegable y seleccione “False”. 

2.9. IDENTIDADES DEL GRUPO DE APLICACIONES

El siguiente paso define el procedimiento para la modificación de las identidades de una aplicación las cuales deben modificarse con la aplicación del ENS para la categoría básica sobre IIS 10 y evitando el uso de identidades de servicio integradas tales como servicio local o sistema local.

Para una mayor seguridad los grupos de aplicaciones deben ejecutarse bajo la identidad del grupo cuando se crea el grupo de aplicaciones, el valor predeterminado y más seguro es "ApplicationPoolIdentity". El uso de una cuenta personalizada es aceptable, pero debe asegurarse de usar una cuenta diferente para cada grupo de aplicaciones.

Paso	Descripción
101.	Inicie sesión en el servidor independiente donde tiene instalado el rol de IIS 10. Pulse sobre el administrador del servidor. 
102.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración.
103.	Inicie la herramienta "Administrador de Internet Information Services (IIS)". Para ello, pulse sobre el menú superior de la derecha de la herramienta "Administrador del servidor" y seleccione: **"Herramientas → Administrador de Internet Information Services (IIS)"** 
104.	Despliegue el servidor y seleccione la opción "Grupos de aplicaciones". 

Paso	Descripción
105.	A continuación, seleccione la aplicación que desea configurar y haga clic botón derecho sobre ella y pulse “Configuración avanzada…”. 
106.	Localice la opción “Identidad” dentro de “Modelo de proceso”. 
107.	A continuación, seleccione la opción que más se adecue a sus necesidades y pulse aceptar. 

2.10. LIMPIEZA DE METADATOS

Se ha de tener en consideración que en un servidor web se pueden alojar documentos que pueden contener información oculta en los metadatos los cuales contienen información que permite catalogar, ordenar y clasificar nuestros archivos, por lo que pueden ser un riesgo de seguridad para nuestra organización, por lo que hay que tener especial atención en la limpieza de los metadatos de los documentos que se alojan en el servidor web por ello antes de alojar un fichero en el servidor web se ha debido de realizar el procedimiento indicado en MP. INFO. 6. LIMPIEZA DE DOCUMENTOS.

En el proceso de limpieza se ha de tener en consideración que se retiraran todos los datos de los documentos además de la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, con la excepción de la información pertinente para el receptor del documento.

2.11. SOLUCIONES WAF (WEB APLICATION FIREWALL)

Un servidor web puede alojar aplicaciones por lo que es importante un control exhaustivo de estas por ello se han de emplear uno de los elementos principales en la protección de entornos de aplicaciones Web que son los cortafuegos (firewalls) de aplicaciones Web, también conocidos como WAF, Web Application Firewall.

El WAF se encargará de proteger los servidores de aplicaciones web de determinados ataques específicos en Internet además de controlar las transacciones al servidor web de nuestra organización.

Este sistema nos permite evitar probables ataques como:

a) “Cross-site scripting” que consiste en la inclusión de código script malicioso en el cliente que consulta el servidor web.

b) “SQL injection” que consiste en introducir un código SQL que vulnere la Base de Datos de nuestro servidor.

c) “Denial-of-service” que consiste en que el servidor de aplicación sea incapaz de servir peticiones correctas de usuarios.

Algunos sistemas WAF existentes en el mercado también monitorizan las respuestas del servidor, por ejemplo, si en una respuesta, que el servidor web envía al usuario se detectan cadenas que pueden ser identificadas como cuentas bancarias, el WAF lo puede detectar como un posible ataque y denegar la respuesta.

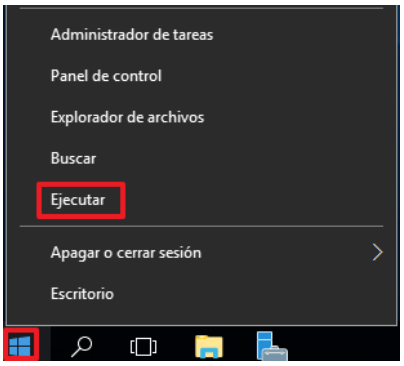
3. GESTIÓN DE ROLES Y/O CARACTERÍSTICAS DEL SISTEMA

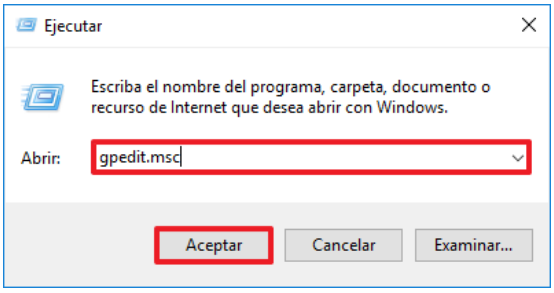
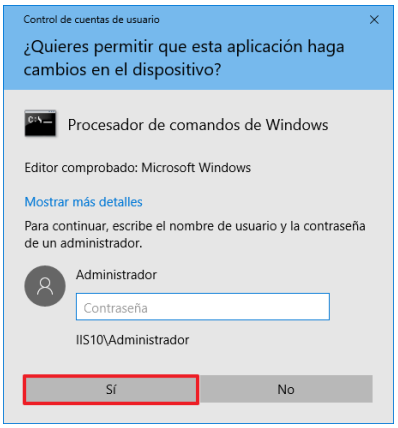
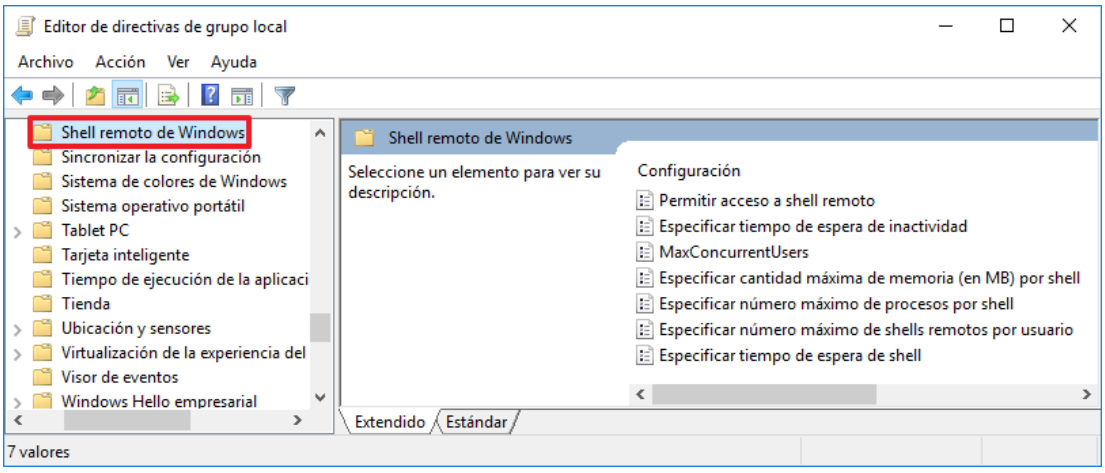
Estos paso a paso se deberán aplicar para instalar o desinstalar roles y/o características implementadas en un servidor independiente, que le sea de aplicación la guía de securización “CCN-STIC-570B - Implementación del ENS en Microsoft Windows Server 2016 Servidor independiente” a partir de la categoría media del ENS.

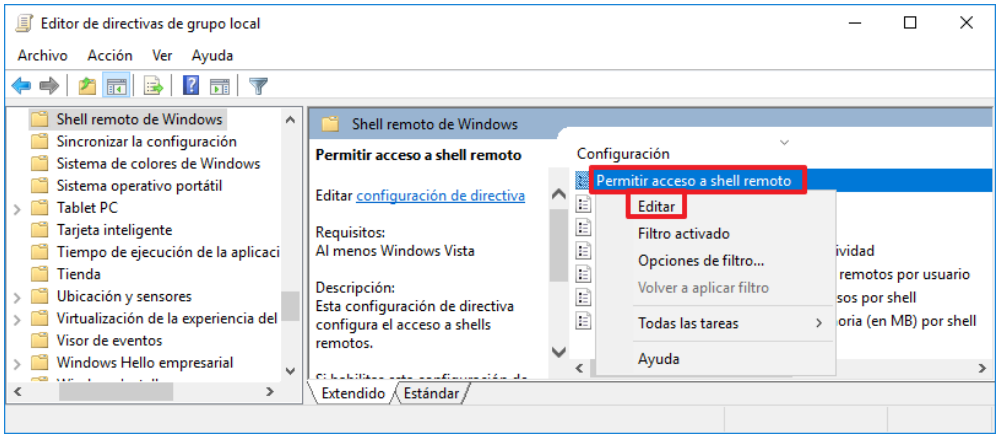
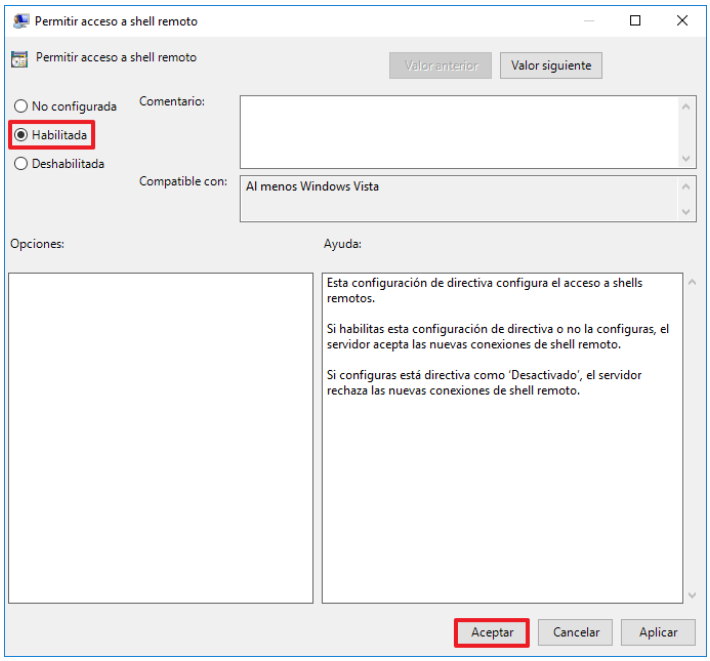
3.1. PREPARACIÓN DEL SERVIDOR INDEPENDIENTE

Para instalar o eliminar un rol y/o característica será necesario la modificación de una directiva de grupo. Los pasos que se describen a continuación se realizarán en el servidor independiente que se está securizando.

Nota: Recuerde que una vez instalados o eliminados los roles y/o características necesarias deberá aplicar el paso "3.4 DESHABILITACIÓN DE UNA DIRECTIVA DE GRUPO LOCAL".

Paso	Descripción
108.	Inicie sesión en el servidor independiente donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador local del equipo.
109.	Inicie el "Editor de directicas de grupo local" para ello pulse botón sobre el botón de inicio con clic derecho. 
110.	Seleccione la opción del menú contextual "Ejecutar". 

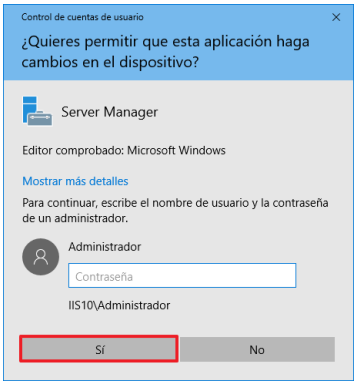
Paso	Descripción
111.	A continuación, escriba el comando “gpedit.msc” y pulse el botón “Aceptar”. 
112.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
113.	Despliegue la política y sitúese en la siguiente ruta: **“Directiva Equipo Local → Configuración del equipo → Plantillas administrativas → Componentes de Windows → Shell remoto de Windows”.** 

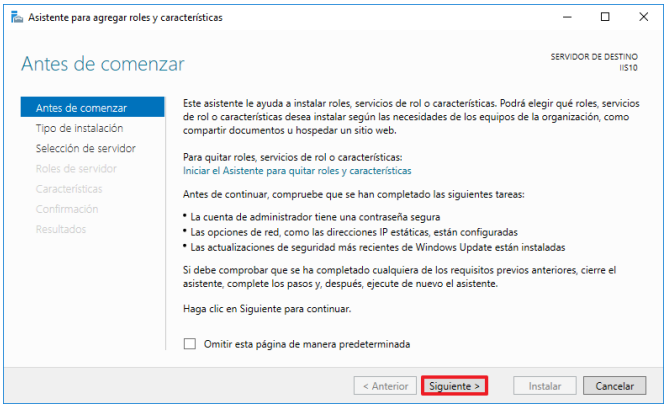
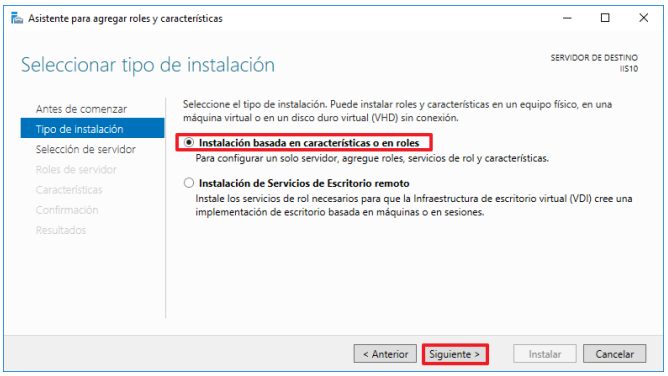
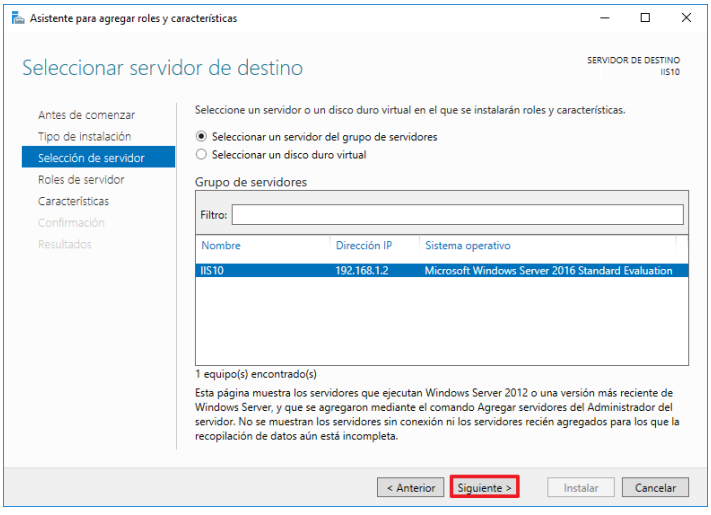
Paso	Descripción
114.	Seleccione la opción “Permitir acceso a Shell remoto”. A continuación, pulse botón derecho y seleccione la opción del menú contextual “Editar”. 
115.	A continuación, marque la opción “Habilitada” y pulse “Aceptar”. 
116.	Para finalizar cierre el “Editor de directivas de grupo local”

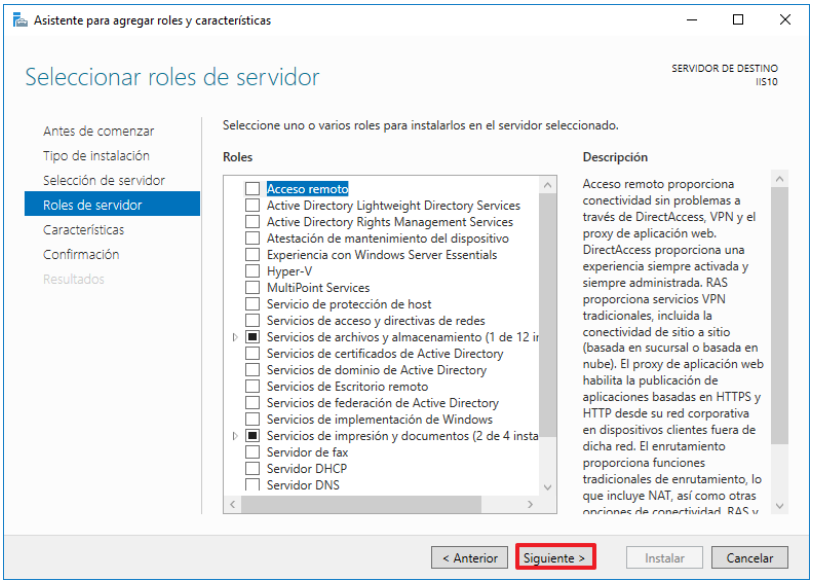
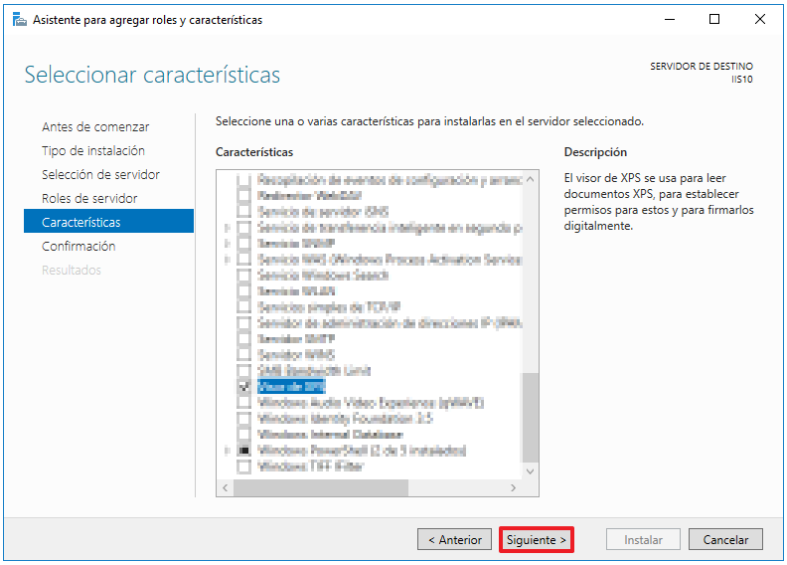
3.2. INSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS

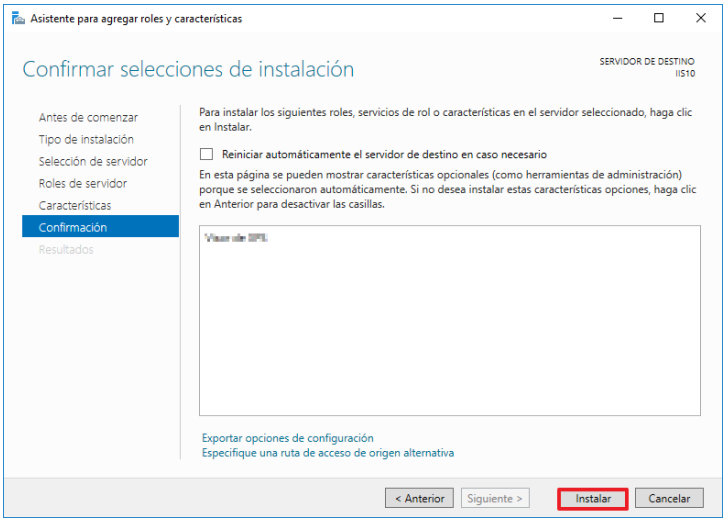
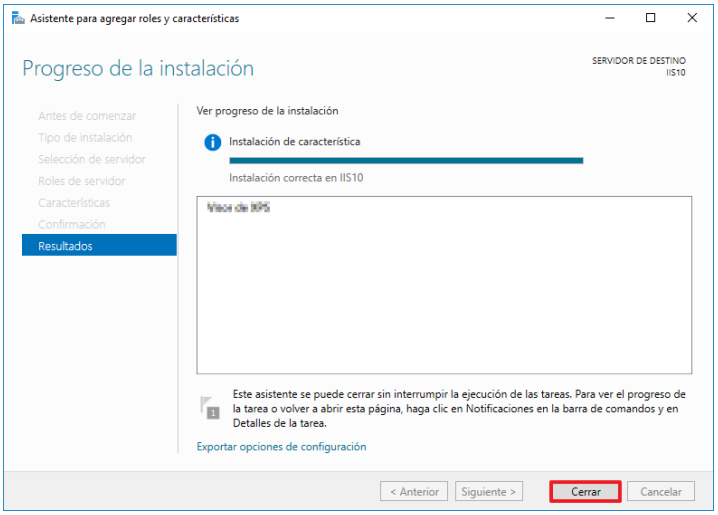
Los pasos que se describen a continuación se realizarán en el servidor independiente que se está securizando.

Nota: Para continuar este paso a paso debe haber aplicado previamente el punto "3.1 PREPARACIÓN DEL SERVIDOR INDEPENDIENTE".

Paso	Descripción
117.	Inicie sesión en el servidor independiente donde vaya a instalar un rol y/o característica.  **Nota:** Inicie sesión con una cuenta que sea administrador local del equipo.
118.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
119.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. 
120.	A continuación, pulse sobre el botón "Administrar" y seleccione la opción "Agregar roles y características". 

Paso	Descripción
121.	Comenzará el asistente para agregar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 
122.	Seleccione el tipo de instalación, “Instalación basada en características o roles” y pulse “Siguiente >” para continuar. 
123.	Seleccione el servidor sobre el cual desea instalar un rol o una característica, y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “IIS10”.

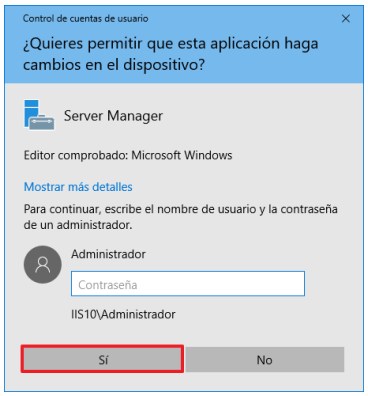
Paso	Descripción
124.	En la siguiente ventana, seleccione los roles que desee instalar en el sistema y pulse “Siguiente >”. 
125.	A continuación, en la siguiente ventana podrá seleccionar las características que desee instalar en el sistema. Seleccione aquellas que desee instalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se instala una característica de prueba, deberá adaptar este paso a los requerimientos de su organización.

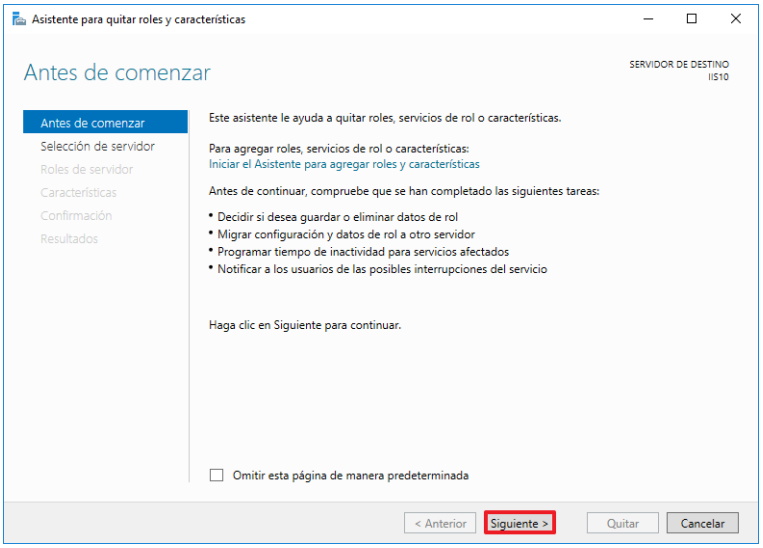
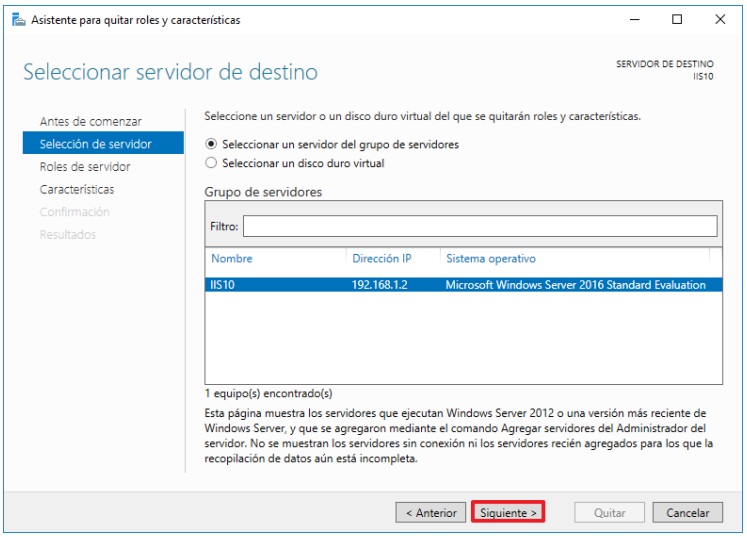
Paso	Descripción
126.	En la ventana “Confirmación” pulse “Instalar” para iniciar el proceso. 
127.	Una vez finalizado el proceso de instalación, pulse sobre “Cerrar” para finalizar la instalación.  **Nota:** En caso de ser necesario, el servidor requerirá un reinicio para finalizar la instalación de roles y características.
128.	Una vez finalizada la instalación de roles y/o características, deberá aplicar el siguiente paso “3.4 DESHABILITACIÓN DE UNA DIRECTIVA DE GRUPO LOCAL”.

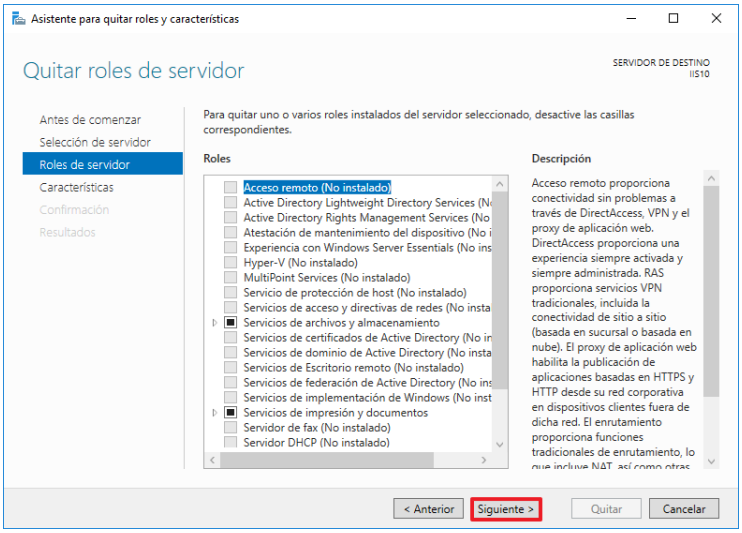
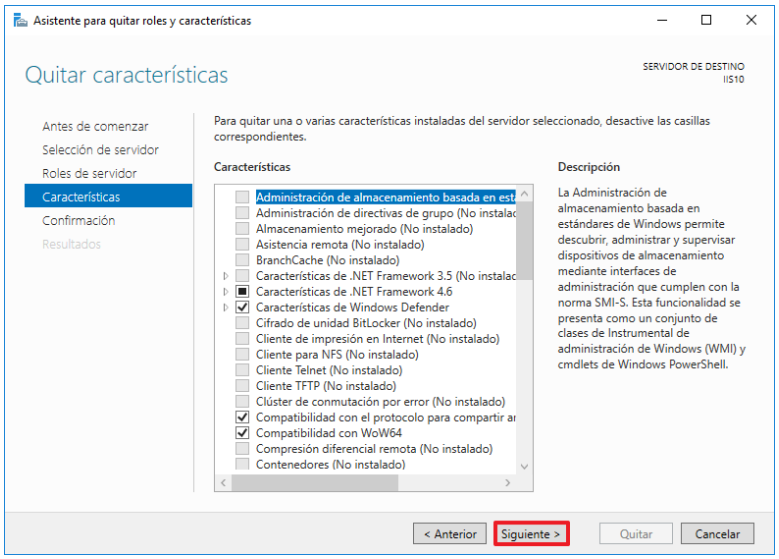
3.3. DESINSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS

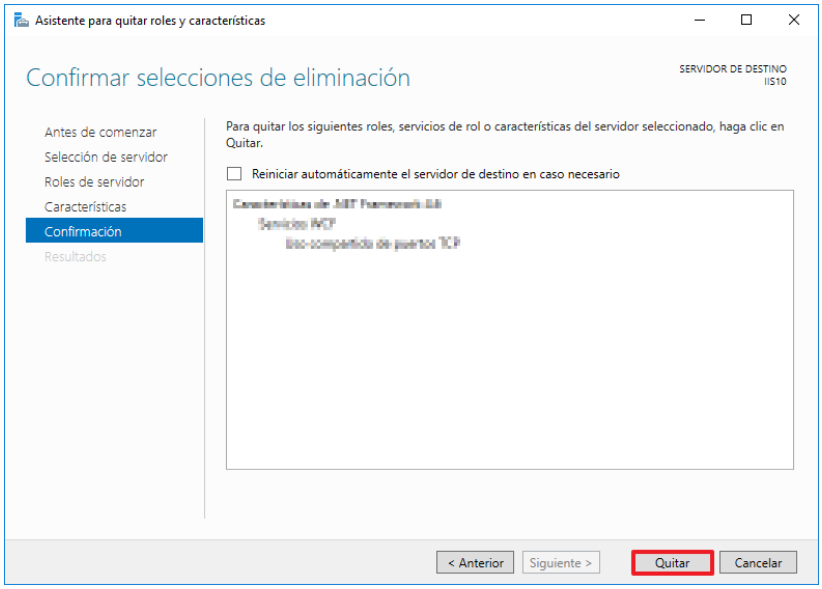
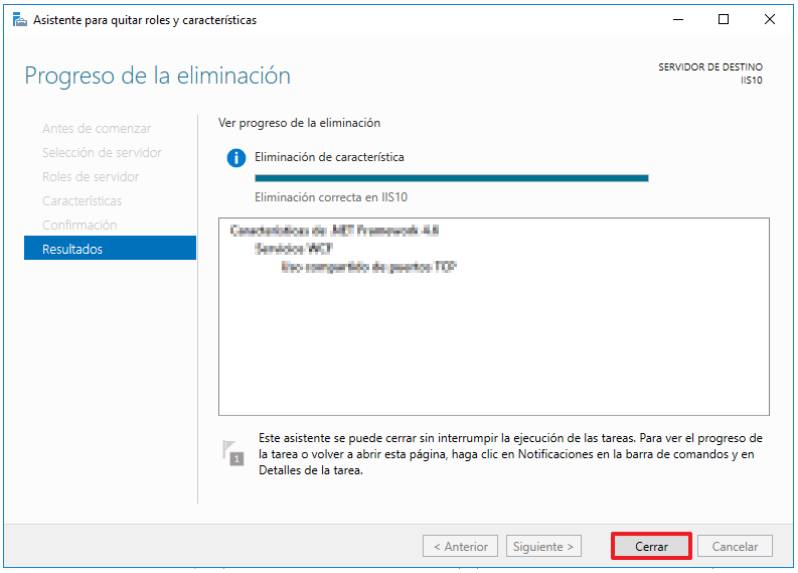
Los pasos que se describen a continuación se realizarán en el servidor independiente que se está securizando.

Nota: Para continuar este paso a paso debe haber aplicado previamente el punto "3.1 PREPARACIÓN DEL SERVIDOR INDEPENDIENTE".

Paso	Descripción
129.	Inicie sesión en el servidor independiente donde vaya a eliminar un rol y/o característica.  **Nota:** Inicie sesión con una cuenta que sea administrador local del equipo.
130.	Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. 
131.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. 
132.	A continuación, pulse sobre el botón "Administrar" y seleccione la opción "Quitar roles y funciones". 

Paso	Descripción
133.	Comenzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 
134.	Seleccione el servidor sobre el cual desea eliminar un rol o una característica y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “IIS10”.

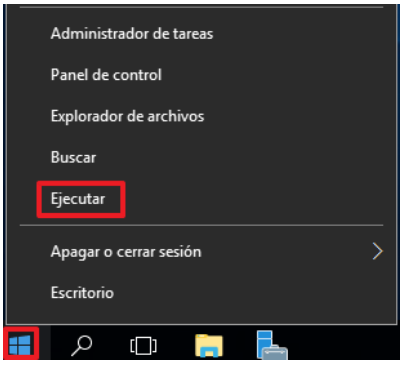
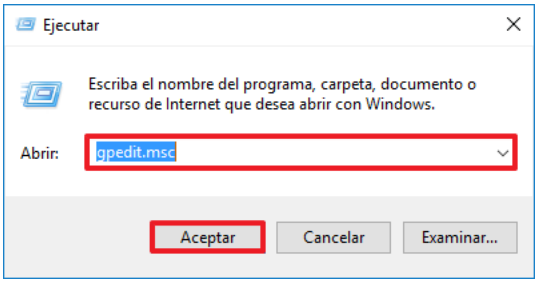
Paso	Descripción
135.	En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Seleccione aquellos que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo no se desinstala ningún rol adicional, deberá adaptar este paso a los requerimientos de su organización.
136.	A continuación, en la siguiente ventana podrá seleccionar las características que desee desinstalar del sistema. Desmarque aquellas que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se desinstala una característica de prueba, deberá adaptar este paso a los requerimientos de su organización.

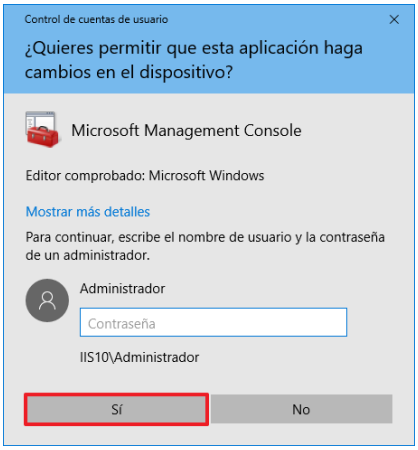
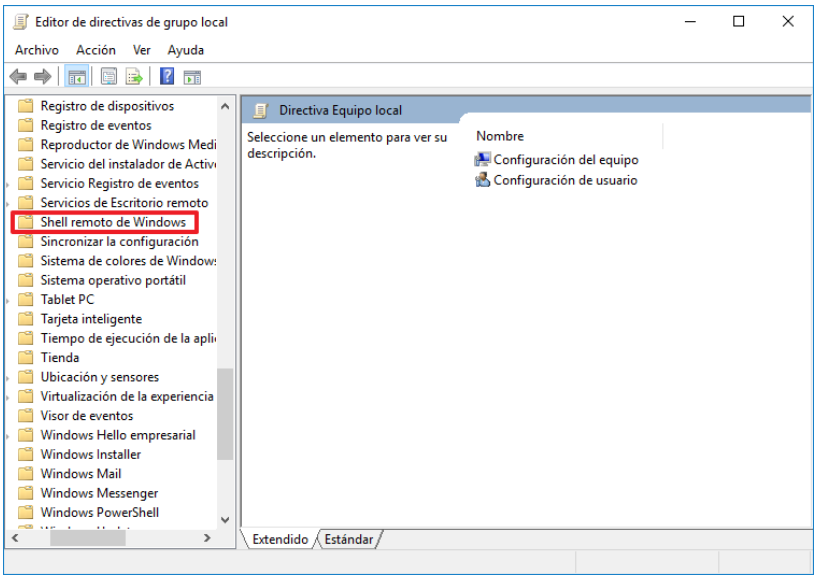
Paso	Descripción
137.	En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso. 
138.	Una vez finalizado el proceso de desinstalación, pulse sobre “Cerrar” para finalizar la desinstalación.  **Nota:** En caso de ser necesario el servidor requerirá un reinicio para finalizar la desinstalación de roles y características.
139.	Una vez finalizada la desinstalación de roles y/o características, deberá aplicar el siguiente paso a paso “3.4 DESHABILITACIÓN DE UNA DIRECTIVA DE GRUPO LOCAL”.

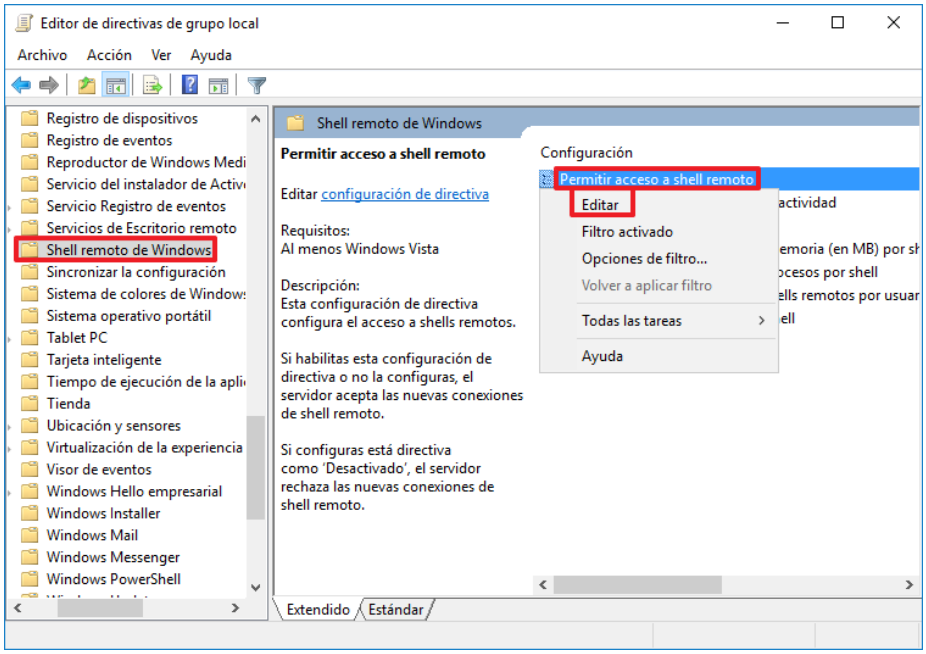
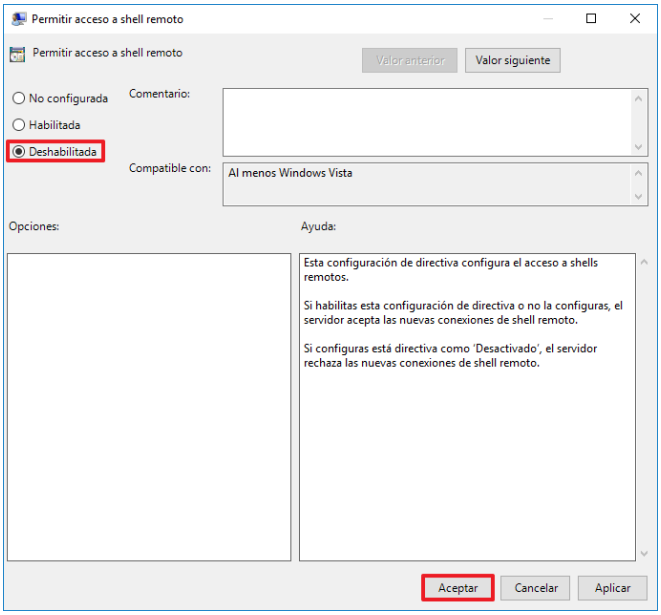
3.4. DESHABILITACIÓN DE UNA DIRECTIVA DE GRUPO LOCAL

Para deshabilitar la directiva de grupo local modificada en el paso “3.1 PREPARACIÓN DEL SERVIDOR INDEPENDIENTE” deberá implementar el siguiente paso a paso.

Los pasos que se describen a continuación se realizarán en el servidor independiente que se está securizando.

Paso	Descripción
140.	Inicie sesión en el servidor independiente donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador local del equipo.
141.	Inicie el “Editor de directicas de grupo local” para ello pulse botón de inicio con clic derecho. 
142.	Seleccione la opción del menú contextual “Ejecutar”. 
143.	A continuación, escriba el comando “gpedit.msc” y pulse el botón “Aceptar”. 

Paso	Descripción
144.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. 
145.	Despliegue la política y sitúese en la siguiente ruta: **“Directiva Equipo Local → Configuración del equipo → Plantillas administrativas → Componentes de Windows → Shell remoto de Windows”**. 

Paso	Descripción
146.	Seleccione la opción “Permitir acceso a Shell remoto” A continuación, pulse botón derecho y seleccione la opción del menú contextual “Editar”. 
147.	A continuación, marque la opción “Habilitada” y pulse “Aceptar”. 
148.	Para finalizar cierre el “Editor de directivas de grupo local”.

ANEXO A.4.4. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA PARA SERVIDORES IIS 10 SOBRE MICROSOFT WINDOWS SERVER 2016 EN UN ENTORNO INDEPENDIENTE

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar la sección de la guía "ANEXO A.4.3 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES IIS 10 INDEPENDIENTES SOBRE MICROSOFT WINDOWS SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA".

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores IIS 10 sobre Microsoft Windows Server 2016 independiente con implementación de seguridad de categoría alta del ENS / Difusión Limitada.

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

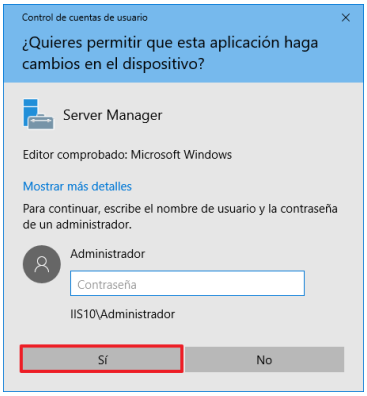
Para realizar las comprobaciones pertinentes en los servidores independientes se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor. Las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

a) Administrador del Servidor

b) Consola de servicios (services.msc)

c) Editor de registro (regedit.exe)

d) Explorador de Archivos (explorer.exe)

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el servidor a comprobar.		En uno de los servidores independientes, inicie sesión con una cuenta que tenga privilegios de administración. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Introduzca credenciales de administrador y pulse "Sí" en la ventana de "Control de cuentas de usuario". 

Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que los servicios del sistema están correctamente configurados		Usando la consola de servicios (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → services.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y pulse "Sí" para continuar. Verifique que el tipo de inicio de los servicios que aparecen en el sistema y en la siguiente tabla coinciden. **Nota:** Dependiendo de las características de IIS 10 instaladas en el equipo es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales.

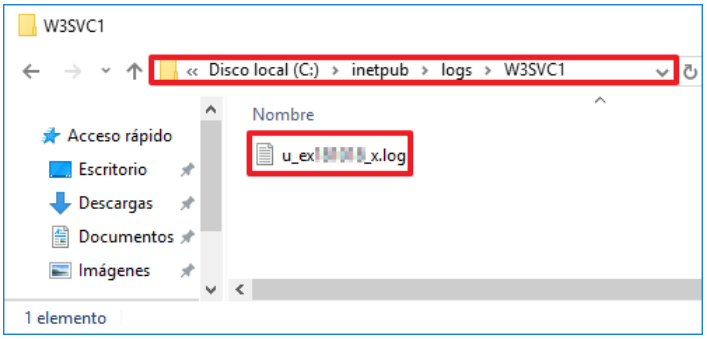
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio auxiliar de host para aplicaciones	AppHostSvc	Automático		
ASP.NET State Service	Aspnet_state	Automático		
Aplicación del sistema COM+	COMSysApp	Manual		
Servicio de administración IIS	IISADMIN	Automático		
Servicio de registro de W3C	w3logsvc	Automático		
Servicio de publicación World Wide Web	w3svc	Automático		
Servicio WAS	WAS	Automático		
Servicio de Administración Web	WMSVC	Manual		

3. Verifique que se han asignado los permisos correctos en el sistema de archivos		Utilizando el Explorador de Windows: **"Windows+R → Explorer"** En caso de no saber dónde apunta cada una de las rutas abreviadas que se especifica, ejecute Explorer <<ruta>> donde <<ruta>> se sustituirá por la ruta abreviada. **Nota:** Para verificar los permisos de cada fichero o carpeta deberá abrir las propiedades del objeto, marcándolo con el botón derecho y eligiendo la opción "Propiedades" del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá situarse en la pestaña "Seguridad". En la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios. Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados.

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		**Usuario**	**Permiso**	**OK/NOK**
%SystemRoot%\inetsrv\MetaBack		Administrador	Control total	
		System	Control total	
%SystemRoot%\LogFiles		Administrador	Control total	
		System	Control total	
		Creator Owner	Control total	

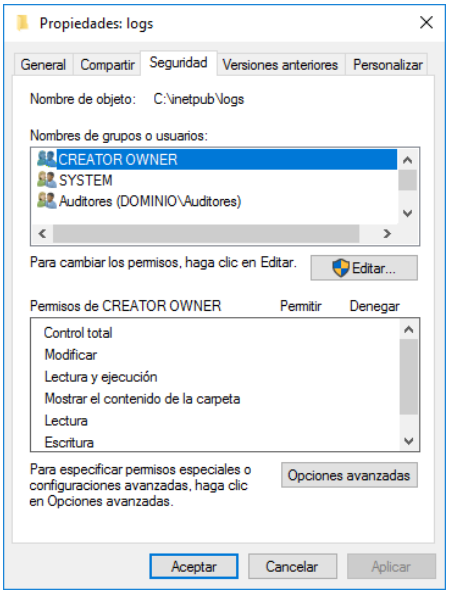
4. Compruebe que el registro de acceso de IIS está operativo.

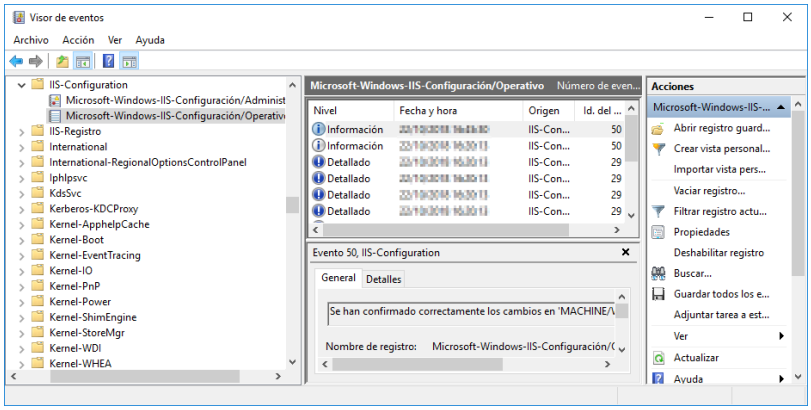
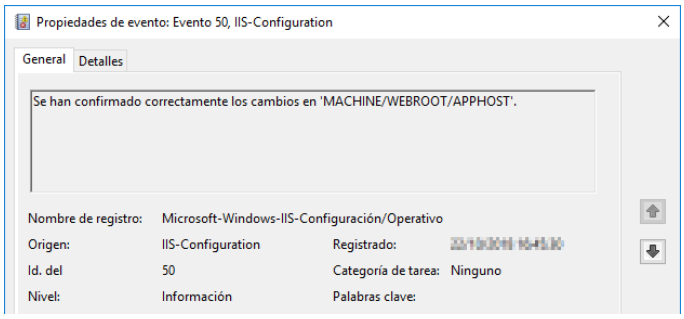
En la configuración que ha realizado ha habilitado el registro de acceso al servidor, por lo que debe asegurarse que está registrando la actividad. Para ello verifique que el directorio **C:\inetpub\logs\W3SVC1** contiene ficheros con el formato **u_ex*fecha*.log**. Abriendo el último deberá ver que registra los accesos correctamente.

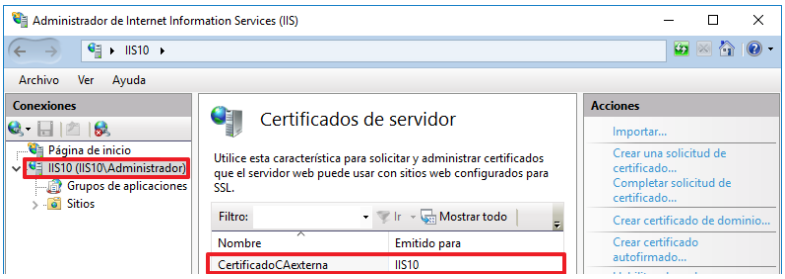
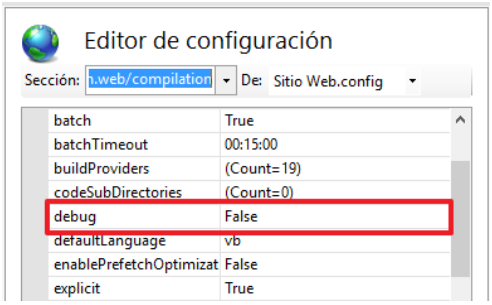
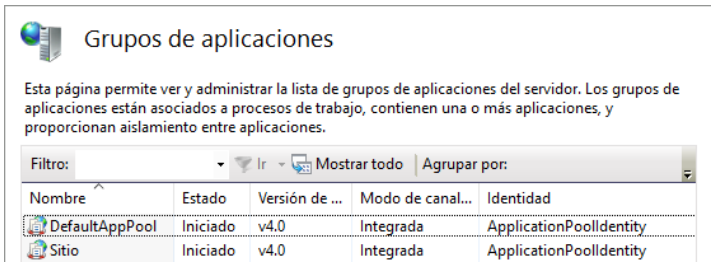


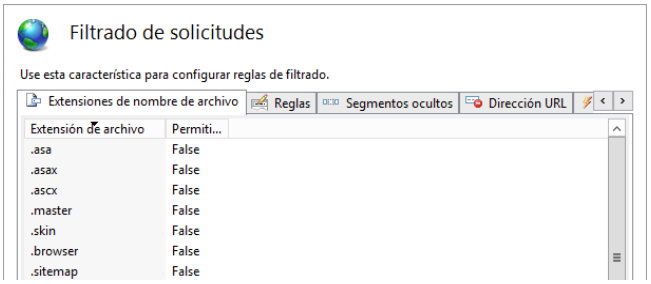
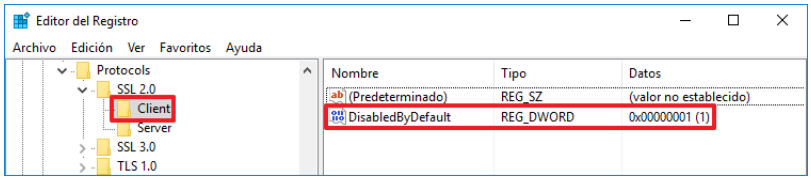
Nota: Tenga en cuenta que no se crea ningún registro hasta que no se realiza alguna actividad.

Ubíquese en la carpeta “logs”, para ello vaya Compruebe los permisos de la carpeta “logs”, únicamente el grupo Auditores además del sistema deben tener acceso.



Comprobación	OK/NOK	Cómo hacerlo
5. Verifique que los registros de Windows están habilitados		Los registros de aplicaciones y servicios integrados con el sistema operativo deben estar habilitados y almacenando información. Abra el Visor de eventos y busque: **"Menú inicio → Herramientas administrativas → Visor de eventos → Registros de aplicaciones y servicios → Microsoft → Windows → IIS-Configuration"**.  Situándose sobre cada uno de ellos, abra el menú contextual, con el botón derecho del ratón, y compruebe que aparece la opción "Deshabilitar registro", lo cual indica que está habilitado.
6. Verifique que los registros son actuales.		Los dos registros deben contener eventos, abra ambos y compruebe que las últimas fechas de registro son recientes. 

Comprobación	OK/NOK	Cómo hacerlo
7. Comprobación certificado sitio web HTTPS		Dentro del "Administrador de Internet Information Services (IIS)" accedemos a "Certificados de servidor".  **Nota:** No olvide estar posicionado sobre el nombre del servidor y no sobre un determinado sitio o carpeta virtual, ya que todas las comprobaciones que está haciendo desde la consola de administración de IIS están siendo sobre el servidor. Se recomienda el uso de certificados EV en la categoría alta del ENS / Difusión Limitada.
8. Comprobación de la depuración de sistemas en producción.		Compruebe que la depuración en sistemas de producción esta deshabilitada. Para ello chequee: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS) → [nombre_del_servidor] → Sitios → Editor de configuración → Sección: System.web → Compilation → Debug → False"**. 
9. Comprobación de las identidades del grupo de aplicaciones.		Compruebe que en las identidades del grupo de aplicaciones no hay identidades de servicio integradas. Para ello chequee: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS) → [nombre_del_servidor] → Grupo de aplicaciones"**. 

Comprobación	OK/NOK	Cómo hacerlo
10. Comprobación del filtrado de solicitudes.		Compruebe que está habilitado el filtrado de solicitudes. Para ello chequee: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS) → [nombre_del_servidor] → Filtrado de solicitudes"**. 
11. Compruebe que se encuentran deshabilitados los algoritmos SSL2, SSL3 y TLS 1.0.		Compruebe que el uso de los algoritmos SSL2, SSL3 y TLS 1.0 estén deshabilitados. Utilizando el Explorador de Windows: **"Windows+R → Regedit.exe"** Y a continuación diríjase a: **"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols"** Compruebe que existen las carpetas con los 3 algoritmos y que contienen las carpetas "Client" y "Server". Compruebe el contenido de la carpeta "Client" tal y como se muestra a continuación.  Compruebe el contenido de la carpeta "server" tal y como se muestra a continuación.