CCN
centro criptológico nacional

Guía de Seguridad de las TIC

IMPLEMENTACIÓN DE SEGURIDAD EN INTERNET INFORMATION SERVICES 10 SOBRE MICROSOFT 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 11:42:56 +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

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

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

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

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

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

2. INTRODUCCIÓN

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

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

Por ejemplo, en el caso de un entorno que le sea de aplicación el ENS, para un servidor miembro de un dominio con Microsoft Windows Server 2016, en el que se instale Microsoft Exchange Server 2013, deberán aplicarse las siguientes guías:

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

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

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

Por ejemplo, en el caso de un entorno de red clasificada, para un servidor con Microsoft Windows Server 2016, en el que se instale Microsoft Exchange Server 2013, deberán aplicarse las siguientes guías:

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

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

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

Nota: Estas guías están pensadas y diseñadas para entornos de máxima seguridad donde no existirá conexión con redes no seguras como puede ser Internet.

3. OBJETO

El propósito de este documento consiste en proporcionar los procedimientos para la implementación y garantía de la seguridad para Internet Information Services 10 (10.0), instalado en un servidor miembro MS Windows Server 2016 perteneciente a un dominio Windows de Directorio Activo.

La presente guía tiene como objeto la implementación de un servidor web estático, dinámico y/o un servidor FTP seguro con IIS 10. Se establecerán también los procesos y tareas administrativas para hacer una administración segura de los mismos.

La instalación y configuración de la solución se ha diseñado de tal forma que la implementación sea lo más restrictiva posible, minimizando la superficie de ataque y por lo tanto los riesgos que pudieran existir. Es posible que para el uso de determinadas funcionalidades de Windows Server 2016 requiera modificar las configuraciones que se plantean con la presente guía. También puede darse el caso que la implementación de otros servicios o aplicaciones, no objeto de esta guía, en el sistema conlleven la modificación de las configuraciones definidas aquí.

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

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

Esta guía asume que IIS 10 se va a implementar sobre un equipo con un sistema operativo Windows Server 2016 Standard de 64 Bits, donde previamente se ha seguido el proceso de implantación definido en la guía “CCN-STIC-570A”.

Así mismo, no se contempla en esta guía la instalación del servicio IIS 10 en clúster, ni se han aplicado características de alta disponibilidad o protección ante fallos del servicio.

4. ALCANCE

La guía se ha elaborado para proporcionar información específica para realizar una implementación del rol de Internet Information Services 10 sobre Microsoft Windows Server 2016 en una configuración restrictiva de seguridad. La guía se ha elaborado para proporcionar información específica sobre cómo implementar las distintas configuraciones para los escenarios planteados en un servidor miembro de un dominio bajo el Sistema Operativo Microsoft Windows Server 2016.

Este documento incluye:

a) **Característica de los servicios de publicación web y FTP seguro**. Completa descripción de los servicios de publicación de sitios web y FTP seguro que proporciona Microsoft para Windows Server 2016.

b) **Riesgos en los sistemas de servidores con IIS**. Completa descripción de los riesgos existentes en una implementación de un servidor web y FTP seguro.

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

d) **Mecanismos para la planificación de configuraciones**. Se incorporan mecanismos para la planificación de las configuraciones de seguridad susceptibles de ello, tales como las plantillas de seguridad.

e) **Guía paso a paso**. Permite implantar y establecer las configuraciones de seguridad en un servidor. Hay una para cada escenario contemplado.

f) **Guía de administración**. Proporciona el método para realizar tareas de administración en el entorno de seguridad establecido.

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

5. DESCRIPCIÓN DE USO DE ESTA GUÍA

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

a) Antes de comenzar a aplicar la guía, además de los requisitos para la instalación del rol de IIS 10, será necesario cumplir los requisitos definidos para Windows Server 2016.

b) Si el entorno en el que está aplicando seguridad pertenece a una red clasificada, se deberá realizar la securización del sistema antes de instalar el rol de IIS 10; será necesario aplicar la guía de seguridad codificada como CCN-STIC-570A y a continuación se deberá instalar y configurar el rol de IIS 10 de Windows Server 2016 tal y como se describe en la presente guía.

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

5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

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

La guía ha sido probada y verificada con la versión de Windows Server 2016 Standard, con los parámetros por defecto de instalación y aplicando la guía "CCN-STIC-570A" para su configuración. No se ha verificado en otros tipos de instalaciones como pudiera ser Windows Server 2016 Datacenter. No obstante, y teniendo en consideración las funcionalidades de ambas versiones de sistema operativo servidor, podría llegar a implementarse la siguiente guía sobre la versión Datacenter. La presente guía no será funcional con la versión Windows Server 2016 Essentials.

Esta guía se ha diseñado para reducir la superficie de exposición de los equipos servidores que cuenten con una implementación de rol Internet Information Services 10 (IIS 10.0) en un entorno de dominio de Active Directory.

La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma de virtualización tipo Hyper-V de Windows Server 2016 con las siguientes características técnicas:

a) Servidor Dell PowerEdgeTM T320:
   i. Intel Pentium Xeon Quad Core.
   ii. HDD 80 GB.
   iii. 32 GB de RAM.
   iv. Interfaz de Red 1 GB.

Esta guía de seguridad no funcionará con hardware que no cumpla con los requisitos de seguridad mínimos de Windows Server 2016. Esto quiere decir que se requieren equipos con procesadores Intel o AMD de 64 bits (x64), con más de 2048 MB de memoria RAM.

Así mismo hay que tener en cuenta que el rol de IIS 10 requiere, para un entorno de producción, un mínimo de requerimientos (2 GB de RAM y 32 GB de espacio de almacenamiento en disco). Oficialmente no se indica ningún requerimiento adicional.

La guía ha sido desarrollada con el objetivo de dotar a la infraestructura de la seguridad máxima en caso de redes clasificadas y la seguridad mínima siguiendo las normas descritas en el ENS. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y por lo tanto pueda ser necesario aplicar acciones adicionales para habilitar servicios o características deseadas en Microsoft Windows Server 2016.

Para garantizar la seguridad de los servidores, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio de Windows Update. Las actualizaciones por lo general se liberan los segundos martes de cada mes, no obstante, hay que tener presente que determinadas actualizaciones por su criticidad pueden ser liberadas en cualquier momento.

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

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

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

5.2 ESTRUCTURA DE LA GUÍA

Esta guía dispone de una estructura que diferencia la implementación del rol de Internet Information Services 10 (IIS 10.0) sobre Microsoft Windows Server 2016 dependiendo del entorno sobre el que vaya a ser aplicado:

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

a) Anexo A: En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows Server 2016 en sus versiones Standard y Datacenter con rol de servidor de ficheros a las necesidades requeridas por el Esquema Nacional de Seguridad (ENS).

b) Anexo B: En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows Server 2016 en sus versiones Standard y Datacenter a las necesidades requeridas en los entornos clasificados donde se quiera instalar el rol de servidor de ficheros.

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

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

6. DESCRIPCIÓN DE INTERNET INFORMATION SERVICES

IIS 10 es la única versión de esta aplicación que funciona sobre Microsoft Windows Server 2016. También se incorpora con el sistema operativo de escritorio Windows 10. En Windows Server 2012 o Microsoft Windows 8 la versión de la aplicación es IIS 8.5.

Internet Information Services proporciona una arquitectura de procesado de las peticiones que incluye:

a) Windows Process Activation Service (WAS), Servicio de Activación de Procesos de Windows, que habilita a los sitios web instalados a que puedan utilizar protocolos distintos a HTTP o HTTPS. Esta característica introducida en IIS 7 permite, por tanto, eliminar la dependencia de HTTP que existía hasta ese momento. IIS 10 también usa el servicio de activación de procesos de Windows para la activación basada en mensajes a través de HTTP. Se puede activar para el entorno .NET 3.5 y .NET 4.6, requiriéndose, en este caso, las características .NET Framework 3.5 y 4.6, respectivamente.

b) Un motor de servidor web que puede ser extendido o reducido poniendo o quitando módulos, tanto los incorporados con el sistema operativo como futuros publicados por Microsoft u otros, como por ejemplo PHP.

c) Dentro del mismo servidor se pueden ejecutar aplicaciones ASP clásicas, ASP.NET o PHP de forma sencilla, por el aislamiento automático de aplicaciones.

d) Plan de procesado de peticiones integrado desde IIS y ASP.NET.

6.1 ARQUITECTURA DE IIS 10

La arquitectura de IIS 10 tiene, entre otras, como características a resaltar:

a) Modularidad;

b) Extensibilidad;

c) Integración ASP.NET;

d) Fácil transporte de la configuración

6.1.1 MODULARIDAD

Todas las características del servidor web son administradas como componentes aislados los cuales pueden ser fácilmente agregados, quitados o remplazados. Esto habilita varias mejoras clave:

a) **Asegurar el servidor por reducción de la superficie de ataque**. La reducción de la superficie de ataque es la mejor forma de asegurar un sistema de servidor. Con IIS se pueden eliminar todas las características de servidor sin uso, dejando al mínimo la superficie de exposición sin dejar de prestar las funcionalidades de las aplicaciones que se quieren servir.

b) **Mejora del rendimiento y reducción del consumo de memoria**. Retirando las características de servidor sin uso se puede reducir la cantidad de memoria que necesita el servidor, y se mejorará el rendimiento al reducir la cantidad de código que se ejecuta en cada petición de una aplicación.

c) **Construcción personalizada / servidores especializados**. Por medio de la selección de las características de servidor, puede construir servidores personalizados que estén optimizados para realizar una función específica dentro de su topología de aplicaciones, tales como almacenamiento en caché de resultados (edge cache) o balance de carga. Se pueden añadir características personalizadas para extender o remplazar cualquier funcionalidad existente utilizando sus propios componentes de servidor o de terceros construidos sobre las nuevas APIs de extensibilidad. La arquitectura modular proporciona beneficios a largo plazo a la comunidad de IIS: facilita el desarrollo de nuevas características según se vayan requiriendo, sea desde el propio Microsoft o por desarrolladores externos.

IIS 10 también se ha modularizado para mejorar el modelo que ya introdujo en IIS 7.0 para la activación de procesos HTTP, ahora se pueden utilizar el servicio de activación de procesos de Windows (WAS) más allá de las aplicaciones Web. Windows Communication Foundation (WCF) se suministra con adaptadores de protocolo que pueden aprovechar las capacidades de la WAS, mejorando la fiabilidad y la utilización de recursos de los servicios de WCF.

6.1.2 EXTENSIBILIDAD

La extensibilidad permite hacer crecer las funcionalidades por medio de nuevos módulos o por sustitución de los existentes. El desarrollo no queda limitado a Microsoft, ya que el entorno de trabajo permite a terceros realizar sus propios módulos sobre IIS 10 y posteriores.

El desarrollo en C++ facilita el desarrollo frente al modelo ISAPI anterior.

Visual Studio facilita el desarrollo, lo que siempre derivará en código más seguro. La integración con IIS se ha profundizado.

Se pueden automatizar o mejorar el uso de módulos tanto en ASP.NET como en C++ nativo en cualquiera de las funcionalidades: monitorización, registro, administración, filtrado de peticiones, redirecciones, etc.

ASP.NET se ha potenciado y puede prestar servicios de manera uniforme a ASP, CGI, archivos estáticos y otros tipos de contenidos.

6.1.3 INTEGRACION A ASP.NET

IIS 10 permite a las aplicaciones web aprovechar las características y la extensibilidad de ASP.NET, incluyendo la autenticación basada en formularios, el estado de sesión y muchas otras. Los desarrolladores pueden utilizar el modelo de extensibilidad de ASP.NET y las API .NET para construir características del servidor IIS, como son las escritas mediante API nativas de C++.

6.1.4 ALMACENAMIENTO DE LA CONFIGURACIÓN TRANSPORTABILIDAD

Desde la versión Internet Information Services 7, el servidor web almacena la configuración en una serie de ficheros en formato XML en vez de una metabase propietaria, como era en versiones anteriores. Estos ficheros, y el estar estructurados en niveles, permite transportar configuraciones de forma rápida, fácil y sin posibilidades de errores por fallos de sincronización o corrupciones de bases de datos.

La edición de los archivos XML de configuración se puede realizar de varias formas, por ejemplo: desde el entorno gráfico, con la herramienta de línea de comandos **AppCMD.exe**, desde Powershell o por medio de un editor de textos (por ejemplo **notepad.exe**).

Los archivos de configuración pueden ser de dos niveles: nivel de servidor o nivel de directorio virtual, directorio físico, aplicación o sitio.

Los ficheros de nivel de servidor son:

a) **Machine.config**. Este archivo se encuentra en la siguiente ruta:

%windir%\Microsoft.NET\Framework\framework_version\CONFIG

b) **Web.config** raíz de .NET Framework. Este archivo se encuentra en la siguiente ruta:

%windir%\Microsoft.NET\Framework\framework_version\CONFIG

c) **ApplicationHost.config**. Este archivo se encuentra en la siguiente ruta:

%windir%\system32\inetsrv\config

La configuración de un directorio virtual o directorio físico, aplicación o sitio pueden almacenarse en una de las siguientes ubicaciones:

a) Archivo de configuración de nivel de servidor.

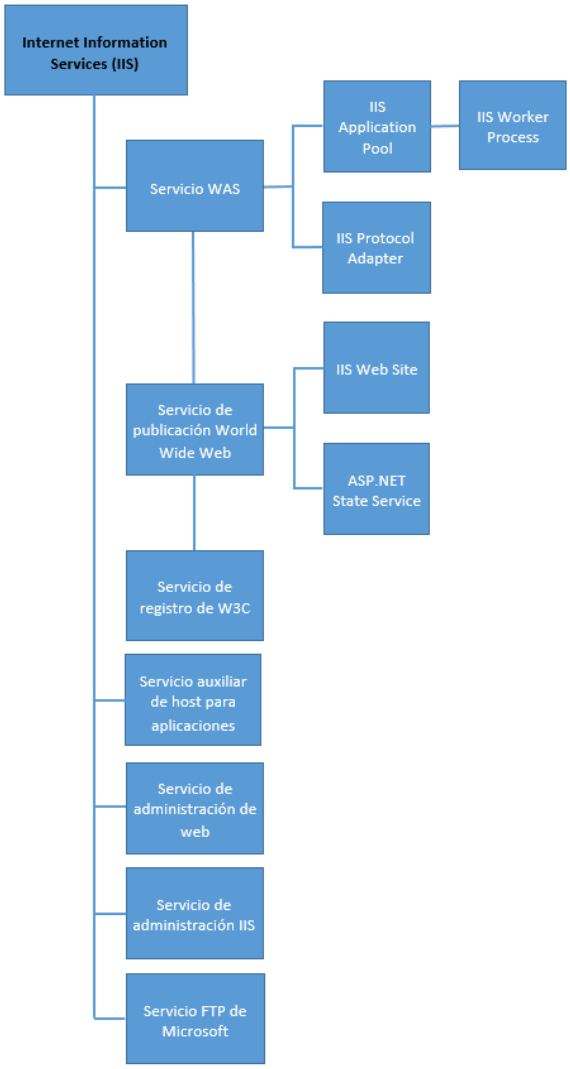
b) Archivo **Web.config** de nivel superior.

c) Archivo **Web.config** para el sitio, la aplicación o el directorio.

Dentro del orden de aplicación de configuraciones, el Web.config propio de un sitio, directorio o aplicación es el último en aplicarse por lo que será el que prevalezca.

6.2 ENTIDADES ADMINISTRATIVAS

Internet Information Services (IIS), es un servidor web escalable, seguro y fiable que proporciona una plataforma de administración fácil para el desarrollo y alojamiento de aplicaciones y servicios web, bajo la jerarquía de entidades administradas, según se muestran en la siguiente imagen:



Jerarquía de entidades administradas

En la siguiente tabla se describen, de una forma sucinta, las entidades.

Descripción	Instalación
Servicio WAS (Windows Process Activation Service)	El servicio de activación de procesos de Windows (WAS) administra la configuración del grupo de aplicaciones y la creación y la duración de los procesos de trabajo para HTTP y otros protocolos. World Wide Web Publishing Service (W3SVC) y otros servicios dependen de WAS.

Descripción	Instalación
IIS Application Pool	Un grupo de aplicaciones de Internet Information Services (IIS) es una agrupación de direcciones URL que se dirige a uno o más procesos de trabajo. Debido a que los grupos de aplicaciones definen un conjunto de aplicaciones web que comparten una o más procesos de trabajo, proporcionan una forma cómoda de administrar un conjunto de sitios y aplicaciones web y de sus procesos de trabajo correspondientes. Los límites del proceso se individualizan para cada proceso de trabajo, por lo tanto, un sitio web o una aplicación en un grupo de aplicaciones no se verán afectados por los problemas de aplicación en otros grupos de aplicaciones. Los grupos de aplicaciones aumentan significativamente la fiabilidad y capacidad de gestión de una infraestructura Web.
IIS Worker Process	Un proceso de trabajo de Internet Information Services (IIS) es un proceso de ventanas (w3wp.exe) que ejecutan las aplicaciones web, y es responsable de tramitar las solicitudes que se envían a un servidor web para un grupo de aplicaciones específico.
IIS Protocol Adapter	Un adaptador de protocolo IIS es un servicio Windows que recibe mensajes sobre un determinado protocolo de red y comunica con WAS para encaminar mensajes entrantes al proceso de trabajo correcto.
Servicio de publicación World Wide Web	El servicio de publicación World Wide Web de Internet Information Services (W3SVC), a veces conocido como servicio WWW, gestiona el protocolo HTTP y contadores de rendimiento HTTP.
IIS Web Site	Un sitio web de Internet Information Services (IIS) es una colección única de páginas Web y aplicaciones Web que está alojado en un servidor Web IIS. Sitios web tienen enlaces que se componen de un puerto, una dirección IP y un nombre o nombres de *host*, esto último opcional.
ASP.NET State Service	Active Server Pages (ASP) permite a los servidores web generar dinámicamente páginas web y crear aplicaciones web interactivas utilizando la tecnología de scripting del lado del servidor.
Servicio de registro de W3C	El seguimiento y registro permiten poder auditar qué ocurre en un servidor, pudiendo personalizarse, activar, desactivar, etc. Para que funcione el servicio de registro de W3C (w3logsvc) debe estar iniciado y así permitir crear un registro para cada sitio.

Descripción	Instalación
Servicio auxiliar de host para aplicaciones	El servicio de apoyo a alojamiento de aplicaciones de Internet Information Services (IIS) permite la configuración del histórico de IIS y el mapeo del grupo de aplicaciones con su SID (identificador de seguridad). Habilita la configuración de la funcionalidad de histórico al guardar el archivo ApplicationHost.config en subdirectorios separados por fechas a intervalos establecidos.
Servicio de administración de web	El Servicio de Administración Web de Internet Information Services (IIS) (WMSvc.exe) permite la administración remota y delegada de un servidor web y sus sitios y aplicaciones web. En entornos de alta seguridad se podría deshabilitar, excepto cuando la gestión remota gráfica sea indispensable. Que este servicio no esté disponible no impide la gestión por otros medios, como PowerShell, aunque, también, podría depender de otros servicios.
Servicio de administración IIS	El servicio IISADMIN aloja el componente de compatibilidad de configuración de IIS 6.0 (metabase). Se requiere la metabase para ejecutar secuencias de comandos administrativos de IIS 6.0, SMTP y FTP.
Servicio FTP de Microsoft	El servicio FTP de IIS permite al servidor web operar como un servidor File Transfer Protocol (FTP). Si el servicio está parado el servidor no puede funcionar como servidor FTP.

Estas “entidades administradas”, descritas en la tabla anterior se instalan como módulos o conjuntos de módulos, como se detalla más adelante.

6.3 DESCRIPCION DE LOS SERVICIOS DE ROL

La versión IIS 10 permite la instalación de módulos, también llamados servicios de rol, de forma individualizada dentro del rol en sí. Estos servicios de rol pueden ser los propiamente incluidos con el sistema operativo, descritos más adelante u otros que desarrolle el fabricante Microsoft en el futuro e incluso de terceros. Esta mejora incorporada en IIS 7 permite minimizar la superficie expuesta al no tener que instalar o activar ningún módulo que no sea necesario.

Los módulos, o componentes, incorporados con el sistema operativo Windows Server 2016 se describen en las tablas de las siguientes secciones. Como se puede observar en la columna “Instalación” no todos se instalan por defecto. En esta guía se instalarán, véanse los anexos de paso a paso, los mínimos indispensables para los distintos requerimientos. De esta forma se reduce la superficie de exposición, pero también se debe tener en cuenta que se reducen las posibilidades y funcionalidades del servicio.

En las siguientes descripciones se han agrupado los módulos por funcionalidad y en el mismo orden que en el que se muestran en la interfaz gráfica de instalación. Entre paréntesis se indica el nombre del parámetro cuando se invoca desde PowerShell.

Las descripciones de cada módulo son las proporcionadas por el fabricante Microsoft. Por ellas se puede deducir la importancia de la experiencia de usuario y la facilidad de trabajo, pero se debe tener en cuenta que en algunas ocasiones entra en contradicción con los sistemas de un nivel de seguridad alto.

Los tres grupos de módulos, completamente independientes, son:

a) Servidor web.

b) Herramientas de administración.

c) Servidor FTP.

6.3.1 DESCRIPCIÓN DE LOS COMPONENTES DEL SERVIDOR WEB

Servidor web proporciona compatibilidad con sitios web HTML y compatibilidad opcional con ASAP.NET, ASP y extensiones de servidor web. Puede usar el rol Servidor web para hospedar un sitio web interno o externo o para proporcionar un entorno en el que los desarrolladores creen aplicaciones web.

Servidor web puede ser invocado por el parámetro de PowerShell Web WebServer.

6.3.1.1 CARACTERÍSTICAS HTTP COMUNES

Características HTTP comunes admite funcionalidad básica de HTTP, como entrega de formatos de archivo estándar y configuración de propiedades de servidor personalizadas. Use Características HTTP comunes para crear mensajes de error personalizados, configurar la respuesta del servidor a solicitudes que no especifican un documento o redirigir automáticamente algunas solicitudes a una ubicación distinta

Estado y diagnóstico puede invocarse por el parámetro de PowerShell Web-Health.

Nombre	Descripción del servicio rol	Instalación
Registro HTTP (Web-Http-Logging)	Registro HTTP proporciona el registro de la actividad del sitio web para este servidor. Cuando se produce un evento registrable (por lo general, una transacción HTTP), IIS llama al módulo de registro seleccionado, que escribe, a continuación, en uno de los registros almacenados en el sistema de archivos del servidor web. Estos registros son adicionales a los que proporciona el sistema operativo.	Predeterminado
Herramientas de registro (Web-Log-Libraries)	Herramientas de registro proporciona una infraestructura para administrar los registros del servidor web y automatizar las tareas de registro comunes.	Disponible

Nombre	Descripción del servicio rol	Instalación
Monitor de solicitudes (Web-Request-Monitor)	Monitor de solicitudes proporciona infraestructura para supervisar el estado de aplicaciones web capturando información sobre solicitudes HTTP en un proceso de trabajo de IIS. Los administradores y programadores pueden utilizar Monitor de solicitudes para entender qué solicitudes HTTP se están ejecutando en un proceso de trabajo cuando este proceso no responde o lo hace muy lentamente	Disponible
Registro de ODBC (Web-ODBC-Logging)	Registro ODBC proporciona una infraestructura que permite registrar la actividad del servidor web en una base de datos compatible con ODBC. Utilizando una base de datos de registro, puede mostrar y manipular mediante programación datos de la base de datos de registro en una página HTML. Puede hacer esto si busca registros para eventos específicos que desee supervisar.	Disponible
Registro personalizado (Web-Custom-Logging)	Registro personalizado proporciona compatibilidad con la actividad de registro de servidor web en un formato que difiere considerablemente de la manera que IIS genera archivos de registro. Utilice Registro personalizado para crear su propio módulo de registro. Los módulos de registro personalizados se agregan a IIS registrando un nuevo componente COM que implementa ILogPlugin o ILogPluginEx.	Disponible
Seguimiento (Web-Http-Tracing)	Seguimiento proporciona una infraestructura para diagnosticar y solucionar problemas de las aplicaciones web. Mediante el seguimiento de solicitudes con error, puede solucionar problemas difíciles de capturar, como un rendimiento insuficiente, o errores relacionados con la autenticación. Esta característica almacena en búfer los eventos de seguimiento para una solicitud y solo los vacía en el disco si la solicitud pertenece a una condición de error configurada por el usuario.	Disponible

6.3.1.2 ESTADO Y DIAGNÓSTICO

Estado y diagnóstico proporciona una infraestructura para supervisar y administrar el estado de servidores, sitios y aplicaciones web, así como para soluciones problemas de los mismos.

Estado y diagnóstico puede invocarse por el parámetro de PowerShell Web-Health.

Nombre	Descripción del servicio rol	Instalación
Registro HTTP (Web-Http-Logging)	Registro HTTP proporciona el registro de la actividad del sitio web para este servidor. Cuando se produce un evento registrable (por lo general, una transacción HTTP), IIS llama al módulo de registro seleccionado, que escribe, a continuación, en uno de los registros almacenados en el sistema de archivos del servidor web. Estos registros son adicionales a los que proporciona el sistema operativo.	Predeterminado
Herramientas de registro (Web-Log-Libraries)	Herramientas de registro proporciona una infraestructura para administrar los registros del servidor web y automatizar las tareas de registro comunes.	Disponible
Monitor de solicitudes (Web-Request-Monitor)	Monitor de solicitudes proporciona infraestructura para supervisar el estado de aplicaciones web capturando información sobre solicitudes HTTP en un proceso de trabajo de IIS. Los administradores y programadores pueden utilizar Monitor de solicitudes para entender qué solicitudes HTTP se están ejecutando en un proceso de trabajo cuando este proceso no responde o lo hace muy lentamente.	Disponible
Registro de ODBC (Web-ODBC-Logging)	Registro ODBC proporciona una infraestructura que permite registrar la actividad del servidor web en una base de datos compatible con ODBC. Utilizando una base de datos de registro, puede mostrar y manipular mediante programación datos de la base de datos de registro en una página HTML. Puede hacer esto si busca registros para eventos específicos que desee supervisar.	Disponible
Registro personalizado (Web-Custom-Logging)	Registro personalizado proporciona compatibilidad con la actividad de registro de servidor web en un formato que difiere considerablemente de la manera que IIS genera archivos de registro. Utilice Registro personalizado para crear su propio módulo de registro. Los módulos de registro personalizados se agregan a IIS registrando un nuevo componente COM que implementa ILogPlugin o ILogPluginEx.	Disponible
Seguimiento (Web-Http-Tracing)	Seguimiento proporciona una infraestructura para diagnosticar y solucionar problemas de las aplicaciones web. Mediante el seguimiento de solicitudes con error, puede solucionar problemas difíciles de capturar, como un rendimiento insuficiente, o errores relacionados con la autenticación. Esta característica almacena en búfer los eventos de seguimiento para una solicitud y solo los vacía en el disco si la solicitud pertenece a una condición de error configurada por el usuario	Disponible

6.3.1.3 RENDIMIENTO

Rendimiento proporciona una infraestructura para el almacenamiento en caché de la salida integrando las capacidades de almacenamiento en caché dinámico de la salida de ASP.NET con las capacidades de almacenamiento en caché estático de la salida existente en IIS 6.0. IIS también permite usar el ancho de banda de forma más eficaz mediante mecanismos de compresión habituales como Gzip y Deflate

Rendimiento puede invocarse por el parámetro de PowerShell Web-Performance.

Nombre	Descripción del sevicio rol	Instalación
Compresión de contenido estático (Web-Stat-Compression)	Compresión de contenido estático proporciona una infraestructura para configurar la compresión HTTP de contenido estático. Esto proporciona un uso más eficaz del ancho banda. A diferencia de las respuestas dinámicas, las respuestas estáticas comprimidas pueden almacenarse en caché sin degradar los recursos de CPU.	Predeterminado
Compresión de contenido dinámico (Web-Dyn-Compression)	Compresión de contenido dinámico proporciona una infraestructura para configurar la compresión HTTP de contenido dinámico. Si se habilita la compresión dinámica, se hace siempre un uso más eficaz del ancho banda, pero si el uso del procesador de su servidor es ya muy alto, la carga de la CPU impuesta por compresión dinámica puede hacer que su sitio funcione muy despacio.	Disponible

6.3.1.4 SEGURIDAD

Seguridad proporciona una infraestructura para proteger el servidor web de usuarios y solicitudes. IIS admite varios métodos de autenticación. Elija un esquema de autenticación apropiado según el rol del servidor. Filtre todas las solicitudes entrantes, rechazando las que coincidan con valores definidos por el usuario sin procesarlas o restrinja las solicitudes según el espacio de direcciones de origen.

Seguridad puede invocarse por el parámetro de PowerShell Web-Security.

Nombre	Descripción del servicio rol	Instalación
Filtrado de solicitudes (Web-Filtering)	Filtro de solicitudes analiza todas las solicitudes que entran en el servidor y las filtra basándose en reglas establecidas por el administrador. Muchos ataques malintencionados comparten características comunes, como direcciones URL muy largas o solicitudes de una acción inusual. Con filtrando las solicitudes puede intentar reducir el impacto de este tipo de ataques.	Predeterminado

Nombre	Descripción del servicio rol	Instalación
Autenticación básica (Web-Basic-Auth)	Autenticación básica proporciona una gran compatibilidad con los exploradores. Adecuado para redes internas pequeñas, raramente se utiliza en Internet público. Su principal inconveniente es que transmite las contraseñas por la red utilizando un algoritmo que se descifra con facilidad. Si se interceptan, estas contraseñas son fáciles de descifrar. Utilice SSL con Autenticación básica.	Disponible
Autenticación de asignaciones de certificado de cliente (Web-Client-Auth)	Autenticación de asignaciones de certificado de cliente utiliza certificados de cliente para autenticar a los usuarios. Un certificado de cliente es un identificador digital de una fuente de confianza. IIS proporciona dos tipos de autenticación mediante la asignación de certificados de cliente. Este tipo utiliza Active Directory para proporcionar asignaciones de certificados uno a uno a través de varios servidores web.	Disponible
Autenticación de asignaciones de certificado de cliente de IIS (Web-Cert-Auth)	Autenticación de asignaciones de certificado de cliente de IIS utiliza certificados de cliente para autenticar a los usuarios. Un certificado de cliente es un identificador digital de una fuente de confianza. IIS proporciona dos tipos de autenticación mediante la asignación de certificados de cliente. Este tipo utiliza IIS para proporcionar asignaciones de certificados uno a uno o de uno a varios. La asignación de certificados nativa de IIS ofrece mejor rendimiento con respecto a la Autenticación de asignaciones de certificado de cliente.	Disponible
Autenticación de Windows (Web-Windows-Auth)	Autenticación de Windows es una solución de autenticación de bajo costo para sitios web internos. Este esquema de autenticación permite a los administradores de un dominio de Windows sacar partido de la infraestructura del dominio para autenticar a los usuarios. No utilice la autenticación de Windows si los usuarios que deben ser autenticados tienen acceso a su sitio web a través de *firewalls* y servidores *proxy*.	Disponible

Nombre	Descripción del servicio rol	Instalación
Autenticación implícita (Web-Digest-Auth)	Autenticación de texto implícita funciona enviando un *hash* de la contraseña a un controlador de dominio de Windows para autenticar a los usuarios. Si necesita una seguridad mejorada con respecto a la autenticación básica, considere la posibilidad de utilizar Autenticación implícita, sobre todo, si los usuarios que deben ser autenticados tienen acceso a su sitio web a través de *firewalls* y servidores *proxy*.	Disponible
Autorización para URL (Web-URL-Auth)	Autorización para URL permite crear reglas que restringen el acceso al contenido web. Puede enlazar estas reglas a usuarios, grupos o verbos de encabezado HTTP. Si configura reglas de autorización para direcciones URL, puede impedir a los usuarios que no sean miembros de determinados grupos tener acceso al contenido o interactuar con páginas web.	Disponible
Compatibilidad con certificados centralizados SSL (Web-CertProvider)	Compatibilidad con certificados centralizados SSL le permite administrar centralmente certificados de servidor SSL mediante un recurso compartido de archivos. El mantenimiento de los certificados de servidor SSL en un recurso compartido de archivos simplifica la administración porque hay un solo lugar para administrarlos. Esta característica se introdujo por vez primera en la versión 8 de IIS.	Disponible
Restricciones de IP y dominio (Web-IP-Security)	Restricciones de IP y dominio permite habilitar o denegar contenido basándose en la dirección IP o nombre de dominio de origen de la solicitud. En lugar de utilizar grupos, roles o permisos del sistema de archivos NTFS para controlar el acceso al contenido, puede especificar direcciones IP o nombres de dominio.	Disponible

6.3.1.5 DESARROLLO DE APLICACIONES

Desarrollo de aplicaciones proporciona una infraestructura para desarrollar y hospedar aplicaciones web. Use estas características para crear contenido web o ampliar la funcionalidad de IIS. Estas tecnologías suelen proporcionar una manera de realizar operaciones dinámicas que generan código HTML, que IIS envía para responder a solicitudes de clientes.

Desarrollo de aplicaciones puede invocarse por el parámetro de PowerShell Web-App-Dev.

Nombre	Descripción del servicio rol	Instalación
ASP (Web-ASP)	Páginas Active Server (ASP) proporciona un entorno de *scripting* de servidor para generar sitios web y aplicaciones web. ASP, que ofrece mayor rendimiento que los *scripts* CGI, proporciona a IIS con compatibilidad nativa con VBScript y JScript. Utilice ASP si tiene aplicaciones existentes que requieren compatibilidad con ASP. Para nuevos desarrollos, considere la posibilidad de utilizar ASP.NET.	Disponible
ASP.NET 3.5 (Web-Asp-Net)	ASP.NET proporciona un entorno de programación orientado a objetos de servidor para crear sitios y aplicaciones web con código administrado. ASP.NET no es simplemente una nueva versión de ASP. ASP.NET se ha rediseñado completamente para proporcionar una infraestructura robusta para compilar aplicaciones web y ha sido reestructurado por completo con el fin de proporcionar una experiencia de programación muy productiva basada en .NET Framework. Esta característica se introdujo por vez primera en la versión 8 de IIS.	Disponible
ASP.NET 4.5 (Web-Asp-Net45)	ASP.NET proporciona un entorno de programación orientado a objetos de servidor para crear sitios y aplicaciones web con código administrado. ASP.NET 4.5 no es simplemente una nueva versión de ASP. Se ha rediseñado completamente para proporcionar una infraestructura robusta para compilar aplicaciones web y ha sido reestructurado por completo con el fin de proporcionar una experiencia de programación muy productiva basada en .NET Framework.	Disponible
CGI (Web-CGI)	La interfaz CGI (Common Gateway Interface) define cómo pasa información un servidor web a un programa externo. Entre los usos típicos está emplear un formulario web para recopilar información y pasarla luego a un *script* CGI que se envía por correo electrónico a otra parte. Dado que CGI es un estándar, los *scripts* CGI se pueden escribir mediante diversos lenguajes de programación. El inconveniente que tiene utilizar CGI es la disminución del rendimiento.	Disponible

Nombre	Descripción del servicio rol	Instalación
Extensibilidad de .NET 3.5 (Web-Net-Ext)	Extensibilidad de .NET permite a los programadores de código administrado cambiar, agregar y ampliar la funcionalidad del servidor web en la canalización de solicitud, configuración e interfaz de usuario. Los desarrolladores pueden utilizar el familiar modelo de extensibilidad de ASP.NET 3.5 y las completas API de .NET para generar características de servidor web que sean igual de potentes que las que se escriben mediante las API nativas de C++. Esta característica se introdujo por vez primera en la versión 8 de IIS.	Disponible
Extensibilidad de .NET 4.5 (Web-Net-Ext45)	Extensibilidad de .NET permite a los programadores de código administrado cambiar, agregar y ampliar la funcionalidad del servidor web en la canalización de solicitud, configuración e interfaz de usuario. Los desarrolladores pueden utilizar el familiar modelo de extensibilidad de ASP.NET 4.5 y las completas API de .NET para generar características de servidor web que sean igual de potentes que las que se escriben mediante las API nativas de C++. Esta característica se introdujo por vez primera en la versión 8 de IIS.	Disponible
Extensiones ISAPI (Web-ISAPI-Ext)	Las extensiones de la Interfaz de programación de aplicaciones para servidores de Internet (ISAPI) proporcionan compatibilidad para el desarrollo de contenido web dinámico con extensiones ISAPI. Una extensión ISAPI se ejecuta como cualquier otro archivo HTML estático o archivo ASP dinámico cuando se solicita. Puesto que las aplicaciones ISAPI son código compilado, se procesan de manera mucho más rápida que los archivos ASP o los archivos que llaman a componentes COM+.	Disponible
iltros ISAPI (Web-ISAPI-Filter)	Los filtros de la Interfaz de programación de aplicaciones para servidores de Internet (ISAPI) proporcionan compatibilidad para aplicaciones web que utilizan filtros ISAPI. Los filtros ISAPI son archivos que pueden ampliar o cambiar la funcionalidad proporcionada por IIS. Un filtro ISAPI revisa cada solicitud realizada al servidor web, hasta que encuentra una que debe procesar.	Disponible
Inclusión del lado servidor (Web-Includes)	Inclusiones del lado servidor (SSI) es un lenguaje de *scripts* que se utiliza para generar dinámicamente páginas HTML. El *script* se ejecuta en el servidor antes de que se entregue la página al cliente y normalmente esto implica insertar un archivo en otro. Por ejemplo, puede crear un menú de navegación HTML y utilizar SSI para agregarlo dinámicamente a todas las páginas de un sitio web.	Disponible

Nombre	Descripción del servicio rol	Instalación
Inicialización de aplicaciones (Web-AppInit)	Inicialización de aplicaciones realiza costosas tareas de inicialización de aplicaciones web antes de servir páginas web. Esta característica se introdujo por vez primera en la versión 8 de IIS, aunque estaba disponible como módulo externo en la 7.5.	Disponible
Protocolo WebSocket (Web-WebSockets)	IIS 10 y ASP.NET 4.6 son compatibles con las aplicaciones de servidor de escritura que se comunican mediante protocolo WebSocket. Esta característica se introdujo por vez primera en la versión 8 de IIS.	Disponible

6.3.2 DESCRIPCIÓN DE LOS COMPONENTES DE HERRAMIENTAS DE ADMINISTRACIÓN

Herramientas de administración proporcionan la infraestructura para administrar un servidor web que ejecuta IIS. Puede usar la interfaz de usuario, las herramientas de línea de comando y los scripts de IIS para administrar el servidor web. También puede editar los archivos de configuración directamente.

Las herramientas pueden ser instaladas de forma completamente autónoma o en un equipo con IIS. De igual forma, un servidor IIS no requiere de ninguna herramienta para su funcionamiento.

Nota: Las descripciones que muestra la interfaz gráfica de instalación de los servicios de rol relacionados con las herramientas de administración pueden diferir de las ofrecidas en este manual, las cuales han sido comprobada en los detalles, especialmente de las versiones que se indican.

Nombre	Descripción del servicio rol	Instalación
Consola de administración de IIS (Web-Mgmt-Console)	Administrador de IIS proporciona la infraestructura para administrar IIS 10 mediante una interfaz gráfica de usuario. Puede utilizar el Administrador de IIS para administrar un servidor web local o remoto que ejecute IIS 10, 8.5, 8, 7.5 o 7. Para administrar SMTP debe instalar y usar la consola de administración de IIS 6.	Predeterminado, por sugerencia del asistente
Compatibilidad con la administración de IIS 6 (Web-Mgmt-Compat)	Compatibilidad con la administración de IIS 6 proporciona compatibilidad con versiones posteriores para las aplicaciones y *scripts* que utilizan las dos API de IIS, Objeto base de administración (ABO) e Interfaz del servicio Active Directory (ADSI). Esto le permite utilizar *scripts* existentes de IIS 6.0 para administrar un servidor web de IIS 7, 7.5, 8 ,8,5 u 10.	Disponible

Nombre	Descripción del servicio rol	Instalación
Compatibilidad con la metabase de IIS 6 (Web-Metabase)	La compatibilidad con la metabase de IIS 6.0 proporciona infraestructura para consultar y configurar la metabase a fin de que pueda ejecutar aplicaciones y *scripts* escritos en versiones anteriores de IIS que utilizaban API de Objeto base de administración (ABO) o de Interfaz del servicio Active Directory (ADSI).	Disponible
Compatibilidad con WMI de IIS 6 (Web-WMI)	La compatibilidad con WMI de IIS 6.0 proporciona interfaces de *scripting* de Instrumental de administración de Windows (WMI) para administrar mediante programación y automatizar tareas del servicio web de IIS 10 a partir de un conjunto de *scripts* creados en el proveedor de WMI. Puede administrar sitios con este servicio utilizando las herramientas WMI CIM Studio, Registro de eventos WMI, Visor de eventos WMI y Explorador de objetos WMI.	Disponible
Consola de administración de IIS 6 (Web-Lgcy-Mgmt-Console)	El Administrador de IIS 6.0 proporciona infraestructura para la administración de servidores de IIS 6.0 remotos desde este equipo.	Disponible
Herramientas de scripting de IIS 6 (Web-Lgcy-Scripting)	Herramientas de scripting de IIS 6.0 proporciona la capacidad de seguir usando herramientas de scripting de IIS 6.0 creadas para administrar IIS 6.0 en IIS 7, 7.5, 8 ,8.5.u 10 Esto es especialmente útil si sus aplicaciones y *scripts* utilizan API de Objetos de datos ActiveX (ADO) o de Interfaces del servicio Active Directory (ADSI). Herramientas de scripting de IIS 6 requiere la API de configuración WAS (Windows Process Activation Service).	Disponible
Scripts y herramientas de administración de IIS (Web-Scripting-Tools)	Scripts y herramientas de administración de IIS proporciona la infraestructura para administrar un servidor web de IIS 7, 7.5, 8 ,8.5 u 10 mediante programación utilizando comandos en una ventana de símbolo del sistema o ejecutando *scripts*. Puede utilizar estas herramientas si desea automatizar comandos en archivos por lotes o no desea incurrir en una sobrecarga de administración de IIS utilizando la interfaz gráfica de usuario.	Disponible

Nombre	Descripción del servicio rol	Instalación
Servicio de administración de web (Web-Mgmt-Service)	Servicio de administración proporciona la capacidad de administrar el servidor web en modo remoto desde otro equipo usando el Administrador de IIS.	Disponible

6.3.3 DESCRIPCIÓN DE LOS COMPONENTES DEL SERVIDOR DE PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS (FTP)

Servidor FTP permite transferir archivos entre un cliente y un servidor mediante el protocolo FTP. Los usuarios pueden establecer una conexión FTP y transferir archivos usando un cliente FTP o un explorador web basado en FTP

Nombre	Descripción del servicio rol	Instalación
Servicio FTP (Web-Ftp-Service)	Permite la publicación mediante FTP en un servidor web.	Disponible
Extensibilidad de FTP (Web-Ftp-Ext)	Proporciona compatibilidad para características de extensibilidad de FTP como proveedores personalizados, usuarios de ASP.NET o usuarios del Administrador de IIS.	Disponible

6.4 MEDIOS DE INSTALACIÓN Y ADMINISTRACIÓN DE IIS

Desde la versión 7 de Internet Information Services se han diversificado los medios de configuración, instalación, administración, etc. Las mismas tareas se pueden realizar de formas distintas, lo que permite poder automatizar procesos masivos, generar *scripts* para la administración diaria, crear procesos automáticos para respuesta a ciertos eventos, desinstalar múltiples elementos en múltiples sitios, replicar servidores web con la mera copia de unos cuantos ficheros, etc.

Las herramientas gráficas no están disponibles en la versión server core de Microsoft Server 2016.

Las herramientas de instalación son:

a) Desde **Powershell** se puede utilizar la opción de instalación de roles para instalar un servidor completo o simplemente uno de los módulos, servicios de rol, de IIS.

b) **Pkgmgr.exe** de Windows Server instala paquetes de software, con sus opciones.

c) **Administrador del servidor:** esta herramienta gráfica centraliza la gestión, implementación y administración de todo lo relacionado con IIS, además de otras características del sistema. Permite instalar roles o servicios de rol.

Nota: La herramienta Deployment Image Servicing and Management (DISM) de línea de comandos también permite la instalación de IIS, pero en este caso sobre imágenes del sistema operativo o discos virtuales, por lo que no es objeto de esta guía.

Para la administración del servidor se puede recurrir a múltiples medios y herramientas:

a) Edición directa de los **ficheros XML** de configuración del servidor.

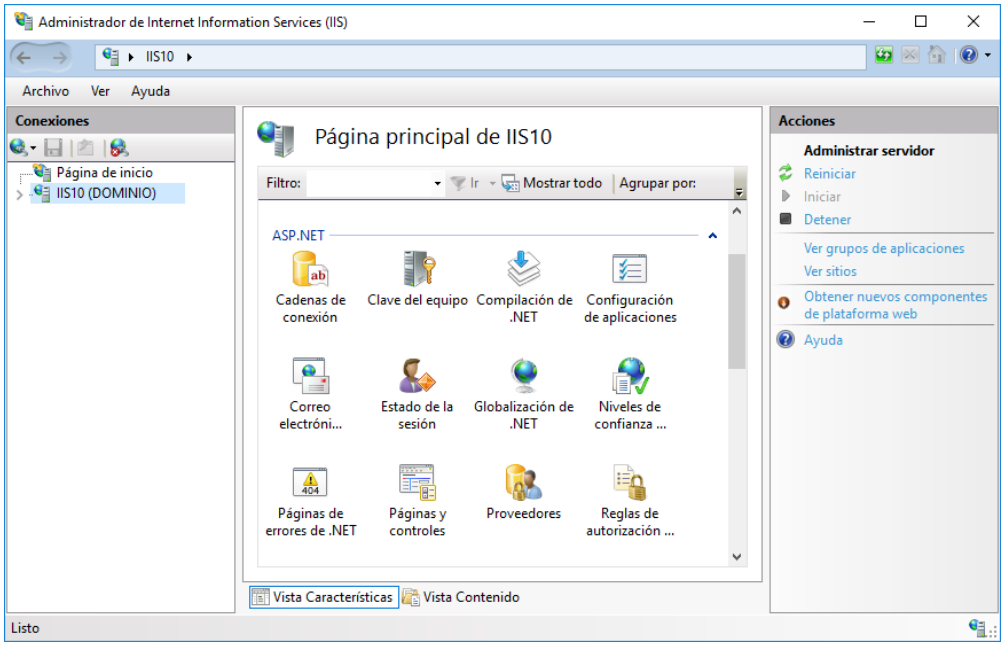
b) **Administrador de Internet Information Services (IIS)**, herramienta gráfica y habitual de gestión de todas las características. Incluye un editor de los ficheros XML de configuración.

c) Herramienta de línea de comando **AppCMD.exe**, alojada en %windir%\system32\inetsrv, para configurar y consultar objetos en el servidor web y para devolver los resultados en formato de texto o XML.

d) Cualquier actuación sobre un sistema Windows, y por tanto sobre IIS, se puede realizar desde **Powershell**. Como se ha indicado más arriba permite instalar y automatizar las instalaciones, pero también administrar el servidor en toda su extensión.

6.5 IMPLEMENTACIÓN DE SITIOS WEB CON ASP EN IIS 10

La instalación de ASP o ASP.NET en un entorno Internet Information Services 10 debe ser planificada de forma adecuada para evitar instalar opciones que no se requieran, o lo contrario. Instalar servicios del rol web server que no se requieran o instalarlos y no configurarlos de forma adecuada expondrán al servidor de una forma innecesaria.

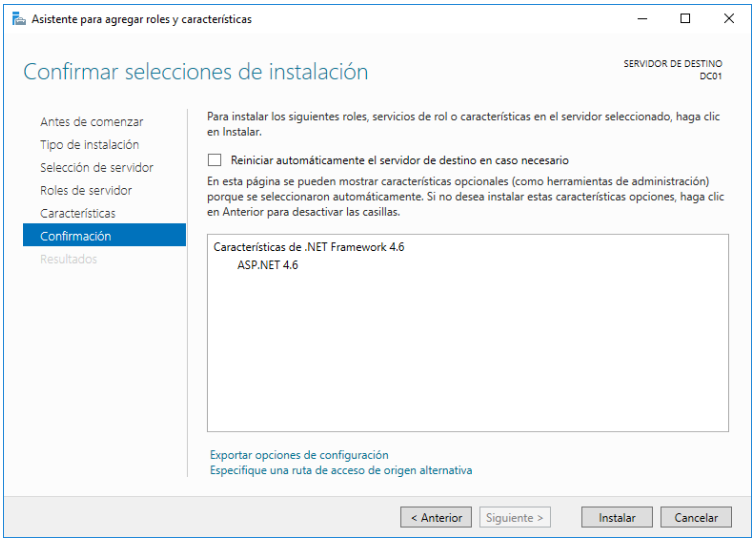


Acceso a algunas de las características configurables de ASP.NET dentro de IIS 10.

La implementación de un sitio ASP.NET requiere una planificación que debe ser realizada entre el equipo de desarrollo del sitio web ASP.NET y los técnicos de seguridad y sistemas.

En IIS 10 se pueden instalar módulos para aplicaciones basadas en ASP 2.0, ASP.NET 3.5 y ASP.NET 4.6. Siempre que la aplicación soporte la posibilidad, se deberá instalar la versión más moderna de ASP, ya que las medidas que implementa de seguridad son mayores (siempre que se configurasen y la programación haya sido acorde a criterios de protección).

IIS 10 permite simultanear aplicaciones con diferentes versiones de framework .NET.



No es posible decidir cuál es la configuración adecuada de forma genérica ya que cada aplicación tiene sus requerimientos y características. Microsoft TechNet, además de otros, ofrece una breve, pero útil guía de implementación, dentro de la cual uno de los pasos es la planificación de un sitio web ASP.NET.

7. SEGURIDAD EN SISTEMAS WEB Y FTP

IIS puede servir dentro de la red corporativa, intranet, o hacia Internet, en cualquiera de los tres casos se deben tomar medidas para asegurar el servicio. Los ataques pueden provenir de usuarios o equipos en la red LAN o desde redes públicas.

Para ofrecer una seguridad completa para los servidores web y las aplicaciones de la intranet de una organización, cada servidor Internet Information Services debe protegerse de:

a) Los ordenadores cliente que puedan conectarse a él.

b) Otros servidores web y aplicaciones que se ejecuten en otros servidores dentro de la intranet corporativa, sean IIS u otros

c) Posibles accesos no autorizados desde redes públicas.

También hay que asegurar el aislamiento de los distintos sitios web o aplicaciones que puedan compartir un único servidor IIS.

Parte de las medidas que se pueden tomar son intrínsecas al servidor donde se aloja IIS, como activar y configurar adecuadamente el firewall de Microsoft Windows Server 2016 e instalar y configurar los módulos de seguridad que proporciona el propio IIS (módulos de filtrado, autenticación y restricciones).

Para tomar una posición proactiva contra los usuarios maliciosos y atacantes, IIS no está instalado por defecto en los miembros de la familia Microsoft Server 2016.

El “Administrador de IIS” es una interfaz gráfica (GUI) diseñada para facilitar la administración de IIS. Incluye los recursos para la administración de sitios, carpetas y la configuración de los grupos de aplicaciones, así como las funciones de seguridad, rendimiento y fiabilidad. Desde la versión IIS 7 no es compatible con versiones anteriores por lo que, si se necesita administrar IIS 6, o versiones inferiores, deberá instalar el módulo de administración que se incluye para ello.

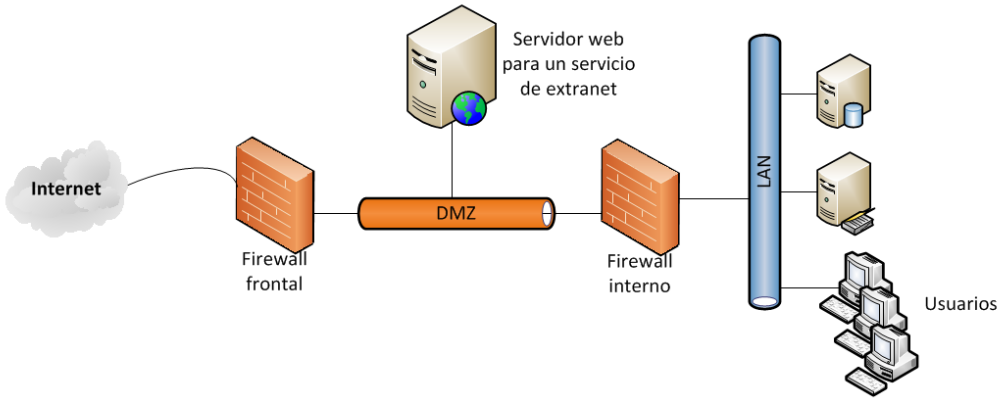
Para utilizar la herramienta de administración de IIS en equipos remotos es indispensable iniciar el servicio de administración de web (WMSvc). Si bien esto se puede considerar una ventaja o comodidad también es una exposición evitable, por lo que en esta guía no se contempla (entre otras medidas, el servicio “WMSvc” se deshabilita desde la directiva de grupo). La forma natural, de los equipos bajo esta implementación, de ser administrados será utilizando las herramientas desde el servidor local.

En esta guía se detallan varias configuraciones que se deben implementar para mejorar la seguridad de los servidores IIS que albergan el contenido HTML de una intranet corporativa o en Internet situados detrás de un firewall. Sin embargo, para garantizar que los servidores IIS permanezcan protegidos, también se deberían implementar procedimientos de supervisión, detección y respuesta.

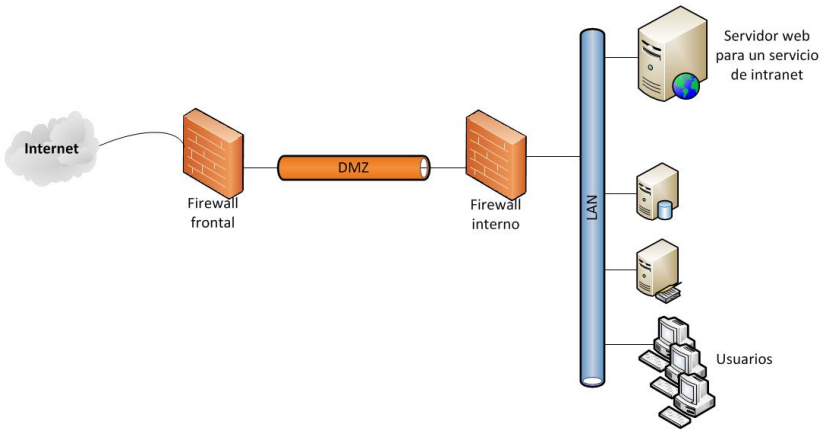
Cuando IIS es parte de un sistema completo de servicio en alta disponibilidad se deberá evaluar la posibilidad de utilizar uno de los medios que provee Microsoft: balanceo de carga en red (NLB) o clúster de conmutación por error. Ninguno de ellos contemplados en esta guía.

Aprovechando la instalación completamente modular podrá ajustar de forma adecuada al uso de cada servidor IIS. Una medida de seguridad de fácil implementación y gran efectividad es instalar solo aquellos módulos que sean indispensables, evitando que no se mantengan o supervisen, además de la reiterada, disminución de la superficie expuesta a posibles ataques.

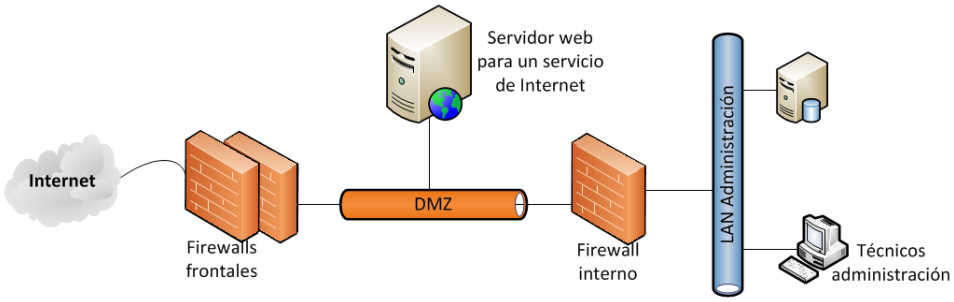
Dependiendo del uso que vaya a darse al servidor (intranet, extranet o Internet) deberá seleccionarse la ubicación en la red, si bien también puede haber otras variables que pueden tener influencia en la topología a implementar.



Ejemplo de topología de red para un servidor web de una extranet.



Ejemplo de topología de red para un servidor web de una intranet.



Ejemplo de servidor web para Internet con dos niveles de protección como exige, por ejemplo, el Esquema Nacional de Seguridad para sistemas de categoría alta.

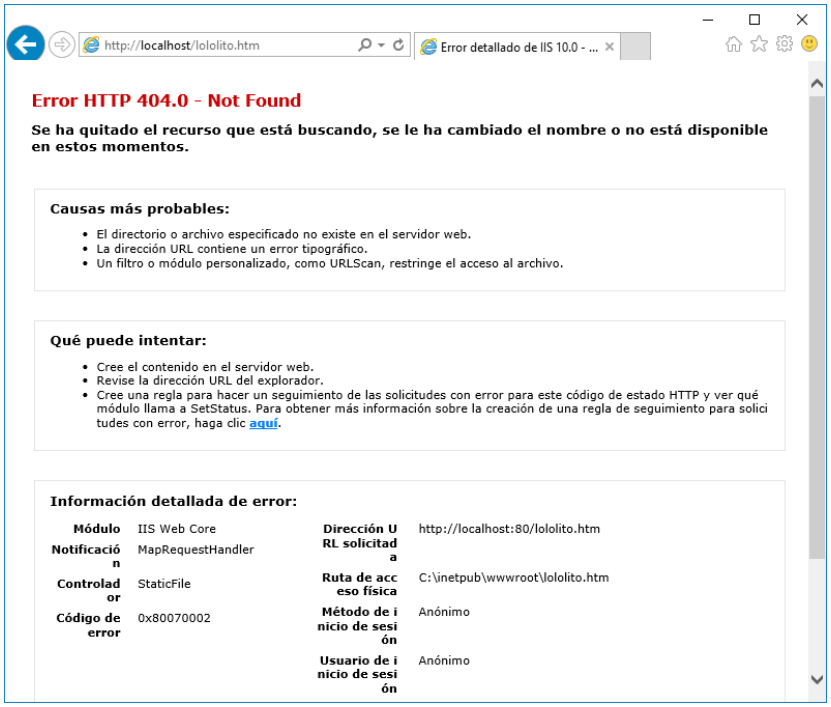
La protección de la información debe estar presente como premisa, por ello nunca se deberá exponer directamente a Internet u otras redes públicas. Si existe una zona intermedia de seguridad, DMZ, tampoco será el lugar para alojar datos, sean bases de datos, ficheros, formularios, etc.

La línea frontal puede ser reforzada con dispositivos tipo firewall, pero diseñados y pensados para proteger servidores web. Se les conoce con el nombre de Web Application Firewalls, WAF.

En la instalación se tratará otro asunto importante, la información que es capaz de ofrecer de forma involuntaria un servidor, por ejemplo, si habilita que el propio servidor ofrezca el documento predeterminado que debe abrirse a un supuesto cliente que accede sin conocimiento preciso, esta funcionalidad facilita la tarea a posibles usuarios desde un punto de vista comercial, pero ofrece una información adicional que, de no conocerse, es un primer nivel de seguridad. De esta forma, será indispensable que quien quiera acceder a nuestro servidor conozca la URL completa y no solo su nombre DNS.

La emisión de páginas de error detalladas ayuda a los administradores en las tareas de resolución de incidencias, pero también ofrece información a posibles atacantes. Se deberán tomar medidas para que dichos avisos sean lo menos informativos posible. Se han dado casos, a lo largo de la historia de la informática, de servidores web que fueron atacados fácilmente porque en sus mensajes de error mostraban la versión del *software* y por tanto daban los datos de vulnerabilidades descubiertas para esa versión concreta.

Mensaje de error detallado por defecto que emite IIS 7.5 ante una petición a un fichero inexistente. Muestra, incluso, el tipo de inicio de sesión.



Mensaje de error detallado por defecto que emite IIS 10 ante una petición a un fichero inexistente. Muestra, incluso, el tipo de inicio de sesión.

7.1 AUDITORIA Y REGISTRO

La auditoría y el registro de la actividad son indispensables para poder realizar tareas de análisis de uso, análisis forense y obtener resultados en pruebas. Para estas tareas dispone de muchas herramientas. Entre otras:

a) Registro de aplicaciones y servicios de Windows.

b) Registro de solicitudes del servidor IIS.

c) Registros de Windows (aplicación, seguridad, sistemas, etc.).

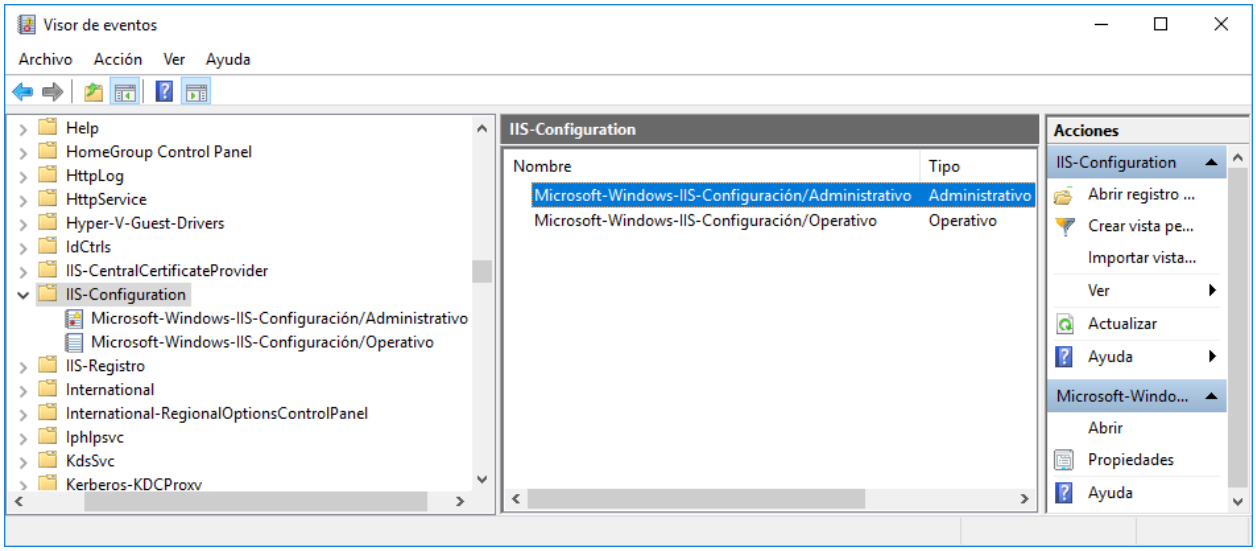
d) Históricos de navegación.

e) Auditoría de ficheros y objetos.

Se entiende que el registro de actividad debe separarse en dos niveles principales: la actividad del servicio como tal y la actividad de los usuarios en su interacción con el servidor. Cada una de ellas se configuran y almacenan de forma independiente.

No es posible crear un modelo para todos los servidores, sino que habrá que adaptarlo a los contenidos, uso y posición del servidor.

El mecanismo de registros de servicios y aplicaciones en Windows Server 2016 a través del sistema ETW (Event Tracing for Windows) incorpora un módulo específico para el servicio de Internet Information Service.



Registro de aplicaciones y servicios de Windows Server 2012.

Para que el registro se active se deberá proceder como se detalla en los anexos donde se describen las instalaciones de los servidores paso a paso.

Una vez configurado, el registro es almacenado en la ruta de disco siguiente %SystemRoot%\System32\Winevt\Logs\ y con sendos ficheros:

a) Microsoft-IIS-Configuration%4Operational.evtx.

b) Microsoft-IIS-Configuration%4Administrative.evtx.

Los eventos administrativos indicarán actuaciones que el administrador tendrá que atender necesariamente mientras que los operacionales recogen aquellos habituales, por ejemplo: inicio o parada del servidor, modificaciones de carpetas virtuales, etc.

Esta característica le permite monitorizar los cambios que sufra la configuración almacenada por medio de mensajes que recogen el cambio realizado, quién lo ha hecho, cuándo, etc. Este registro es equivalente a cuando se activaba la auditoría de la metabase de versiones anteriores.

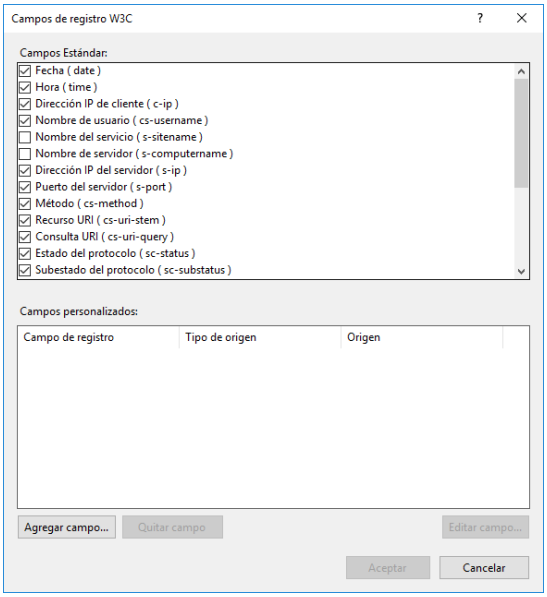
Este elemento le permitirá detectar cambios del servidor, que estén realizados por scripts, usuarios, atacantes o administradores. Pero si se utiliza la herramienta de línea de comandos, **AppCmd.exe**, o similares no se mostrará el identificador de proceso correctamente, aunque sí se podrá ver el autor del cambio.

No se registran en este método aquellos cambios que se realicen de forma directa sobre ficheros de configuración, por ejemplo, si se edita el fichero applicationHost.config directamente con el bloc de notas. En este caso, si fuese necesaria la auditoría en su organización, deberá activarla a nivel del sistema de ficheros.

La activación de estos registros no debería afectar al rendimiento de CPU o RAM de forma considerable ya que utiliza el subsistema ETW de Windows que permite la gestión de miles de eventos por segundo. Para evitar que afecte al rendimiento de disco se puede limitar el tamaño de los ficheros en sus propiedades o ampliarlos si la prioridad es la auditoría frente al rendimiento. Este registro, ETW, es también importante para realizar múltiples tareas de diagnóstico y análisis en caso de error.

Otra forma de auditar el servidor IIS es utilizando el registro de Windows del visor de eventos (sistema y aplicaciones, principalmente).

El registro de actividad del servidor se debe configurar e instalar como un módulo (en el caso del servidor FTP se incorpora de forma predeterminada como parte del servicio). El registro permite acceder a la actividad con selección de qué campos se quieren recoger de cada conexión, o intento de conexión. Desde la versión 8.5 existe la posibilidad de crear campos personalizados que pueden ayudar a hacer un mejor seguimiento.



Lista de campos del registro W3C de IIS 8.5. La lista de campos muestra uno creado, a modo de ejemplo.

Los registros de actividad son guardados en ficheros de texto plano (en el caso seleccionado del formato W3C) que se deben proteger con permisos NTFS. Por defecto se guardan en C:\Intepub\Logs\Logfiles, y para el formato W3C en la subcarpeta W3SVC1, y con el formato u_exaammdd.log (aa=año, mm=mes, dd=día).

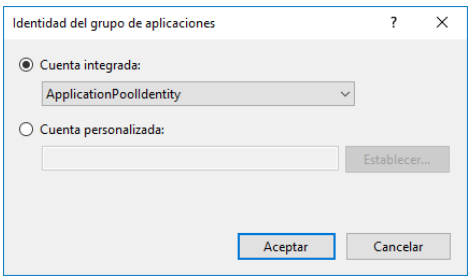
7.2 IDENTIDADES DE GRUPOS DE APLICACIONES

Los grupos de aplicaciones pueden utilizar como identidad una cuenta integrada (LocalService, LocalSystem, NetworkService o ApplicationPoolIdentity) o una cuenta personalizada (local o del dominio).

Nota: El término "identidad", en inglés "identity", puede ser utilizado por Microsoft y en esta guía en referencia a la "Identidad de grupo de aplicaciones" (ApplicationPoolIdentity) o, de forma genérica, a la identidad seleccionada para un grupo de aplicaciones (cuenta del dominio, cuenta integrada de Windows, cuenta local e incluso a la propia identidad de grupo de aplicaciones).

Las identidades de los grupos de aplicaciones (Application pool identities) aportan un nivel de aislamiento mayor respecto a versiones anteriores de IIS, donde dependían de cuentas locales o del dominio de forma exclusiva para la ejecución de los servicios de IIS y de las aplicaciones que sobre este servidor se instalaban.

La identidad de un grupo de aplicaciones es el nombre de la cuenta de servicio con la que se ejecuta el proceso de trabajo de dicho grupo. De manera predeterminada, los grupos de aplicaciones funcionan con ella y se considera el medio más seguro, ya que proporcionando un alto nivel de aislamiento.



Los grupos de aplicaciones utilizan, por defecto, el valor ApplicationPoolIdentity para aislar unos de otros.

Si opta por una de las cuentas integradas que no sea la ApplicationPoolIdentity, debe tener en cuenta: la cuenta de usuario Servicio de red (Networkservice) tiene derechos de usuario de bajo nivel; la cuenta de usuario Sistema local tiene derechos de usuario de nivel superior que las otras dos cuentas de usuario integradas, Servicio de red o Servicio local; y, por último, la ejecución de un grupo de aplicaciones con una cuenta que tiene derechos de usuario de alto nivel supone un grave riesgo para la seguridad.

Las identidades de grupo de aplicaciones no requieren de gestión alguna y no tienen contraseña, lo que facilita su administración y evita problemas de seguridad por falta de mantenimiento.

El aislamiento con cuentas individuales para cada una de las aplicaciones ofrece una garantía de independencia y, especialmente, cuando se aíslan las carpetas con permisos individualizados, aunque sigue siendo inferior a utilizar ApplicationPoolIdentity. Por lo que es conveniente seguir esta serie de recomendaciones:

a) Utilizar un grupo de aplicaciones para cada sitio web o aplicación web.

b) Limitar el acceso a las carpetas y ficheros a la cuenta del grupo de aplicaciones.

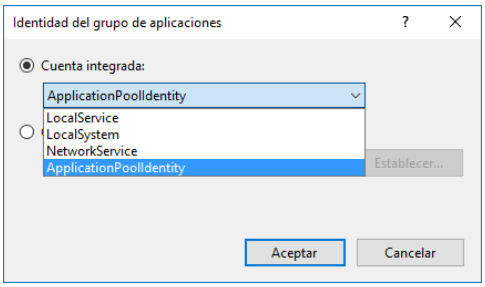
c) Configurar una carpeta temporal ASP.NET independiente para cada sitio y solamente dar acceso a la identidad del grupo de aplicaciones.

d) Asegúrese que la lista de control de acceso de cada raíz de sitio permite el acceso únicamente a su identidad del grupo de aplicaciones.

Cuanto mayor sea el aislamiento entre aplicaciones de sitios mayor es la seguridad ya que en caso de vulnerarse la seguridad de una de ellas no serán accesibles las otras.

Cuando se crea un sitio web automáticamente se crea su aplicación de forma aislada, a no ser que se fuerce el uso de una existente, y se asigna la cuenta integrada ApplicationPoolIdentity.

El uso de identidades frente a otras opciones (usuario IUSR, usuario del dominio, usuario común para todos los sitios, etc.) tiene muchas ventajas, pero no cubre todas las opciones. Por ejemplo, la cuenta de la identidad del grupo de aplicaciones que se crea para cada grupo de aplicaciones, valga la redundancia, es una cuenta local del servidor donde se aloja IIS y eso le impide personarse con permisos del dominio a otros servidores. Esto impide que una aplicación pueda validarse con bases de datos externas al servidor, lo cual requerirá otras soluciones, para dichas interacciones.



Cuentas integradas disponibles para el uso del grupo de aplicaciones.

AUTENTICACIÓN, AUTORIZACIONES, FILTROS, RESTRICCIONES Y PERMISOS

7.2.1 AUTENTICACIÓN

Gran parte de las tareas de mantenimiento e implementación de un servidor Internet Information Services 10 se dedican a asegurar los contenidos. No debe olvidar que servir en una red un recurso siempre es aumentar la superficie de exposición, pero hacerlo en una extranet o incluso públicamente en Internet lleva a extremos la probabilidad de ataque y las posibilidades del mismo. Siempre hay que evaluar y ponderar entre seguridad y servicio, ya que de otra forma puede terminar en cualquiera de los extremos: exposición total sin seguridad a cambio de servicio; recursos casi inaccesibles al preponderar la seguridad. En el término medio debe estar la solución al servicio que debe prestar y con una seguridad adecuada, pero no asfixiante, que impediría el trabajo para el que se sirve el recurso.

Los métodos de autenticación permitirán limitar el acceso a una lista determinada de usuarios (el método por defecto de los servicios web de IIS es la autenticación anónima). No hay que confundir autenticación con permisos u otras restricciones, por ejemplo, puede tener un usuario y contraseña que le permiten acceder a un servidor FTP, sin embargo, no tener permisos de lectura en ninguno de los ficheros.

La autenticación basada en formularios funciona bien para los sitios o aplicaciones en servidores web públicos que reciben numerosas solicitudes. Este modo de autenticación permite administrar el registro y la autenticación de clientes en el nivel de aplicación, en lugar de basarse en los mecanismos de autenticación proporcionados por el sistema operativo.

Al utilizar la suplantación las aplicaciones ASP.NET pueden ejecutarse con la identidad de Windows (cuenta de usuario) del usuario que realiza la solicitud. La suplantación se utiliza normalmente en aplicaciones que confían en Microsoft Internet Information Services (IIS) para autenticar al usuario. De forma predeterminada, la suplantación ASP.NET está deshabilitada. Si la suplantación está habilitada para una aplicación ASP.NET, esa aplicación se ejecuta en el contexto de la identidad cuyo token de acceso pasa IIS a ASP.NET. Ese token puede ser tanto de un usuario autenticado, como para un usuario de Windows que ha iniciado sesión, o el que IIS proporciona para los usuarios anónimos (normalmente, la identidad IUSR_NombredelaMáquina). Se deberá habilitar cuando la aplicación ASP.NET que se instale así lo requiera o admita y se planifique.

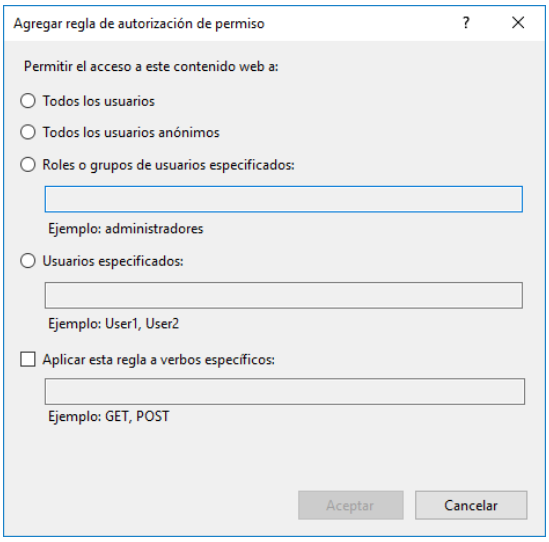
No es posible dar un consejo general para todos los servidores IIS que permita asegurarlos, de ahí la gran variedad de sistemas de autenticación disponibles. Hay que planear el método para cada caso. En los modelos de servidor se ha seleccionado como método de autenticación a instalar el integrado con Directorio Activo (Windows) ya que proporciona facilidad de administración y alta seguridad dentro de un escenario como el que se supone: red local con un bosque o dominio y los equipos servidor y clientes en ella.

En los casos de los servidores de páginas dinámicas ASP.NET se ha incluido la autenticación mediante formularios.

Un método de autenticación adicional es posible instalarlo en cualquier momento para cubrir la necesidad cuando surja por lo que no se recomienda hacerlo en previsión de usos futuros, para minimizar la superficie de exposición durante el intervalo de tiempo sin uso.

7.2.2 AUTORIZACIONES

Las autorizaciones IIS le posibilitan permitir o denegar el acceso a un sitio web a los usuarios en base a su login o su pertenencia a algún grupo. La autorización es independiente de la autenticación, que es la que establece el método de validación.



Puede agregar cuantas reglas sean necesarias para permitir o denegar el acceso.

Las reglas de autorización suelen tener que ser administradas a nivel de sitio y/o carpeta virtual, para poder independizar los accesos en función de su grupo de destinatarios.

Existen reglas de autorización específicas para ASP.NET, si bien el funcionamiento es análogo.

7.2.3 FILTROS

Los filtros de solicitudes permiten controlar las conexiones entre servidor y cliente, restringiendo el comportamiento de protocolos y contenidos.

Se considera una buena práctica de seguridad realizar una configuración básica para el servidor según los usos, situación, contenidos a servir, etc. que se le prevén y luego afinar aún más en cada uno de los sitios que se generen.

El filtrado de solicitudes del servidor web permite crear reglas de filtrado sobre:

a) Extensiones de nombre de archivo: permite crear listas de ficheros, según su extensión, autorizados o denegados.

b) Reglas: para permitir o denegar el acceso al servidor web en función de varios parámetros, como: encabezados, extensiones de servidor y cadenas de denegación.

c) Segmentos ocultos: define la lista de segmentos de dirección URL para los que el módulo de filtrado de solicitudes denegará el acceso y excluirá de las listas de directorios. Un segmento de dirección URL es la parte de la ruta de acceso URL que se encuentra entre los signos de barra diagonal (/).

d) Dirección URL: crea una lista de secuencias de dirección URL para las que el módulo de filtrado de solicitudes denegará el acceso. Por ejemplo, puede especificar "access/config.cfg", lo cual denegará las solicitudes para http://www.estesitio.es/es/access/config.cfg.

e) Verbos HTTP: agrega un verbo a la lista de verbos HTTP para los que el módulo de filtrado de solicitudes permitirá o denegará el acceso. Los verbos también son conocidos como métodos de petición: GET, DELETE, POST, etc.

f) Encabezados: son los encargados de definir los parámetros operativos de una transacción HTTP. Algunos, a modo de ejemplo, son: Content-Type, indica el tipo MIME del cuerpo de la respuesta a un POST o un PUT; Date, fecha y hora a la que se generó el mensaje; Host, nombre del dominio del servidor y el puerto TCP en el cual el servidor está escuchando; etc. Por ejemplo, si creamos una regla Content-Type y un valor de 150, no permitirá encabezados de ese tipo que tengan un tamaño de más de 150 bytes.

g) Cadenas de consulta: permite crear una lista de fragmentos de URL, cadenas de consulta, para los que el módulo de filtrado de solicitudes permitirá o denegará el acceso. Un ejemplo de una cadena de consulta es “name=referrer” dentro de la URL http://www.estesitio.es/cm/app/there?name= referrer.

Los sitios FTP disponen de sistema de filtrado análogo, si bien con menos opciones debido a la naturaleza del protocolo. Las reglas de filtrado aplican a las siguientes características:

a) Extensiones de nombre de archivo.

b) Segmentos ocultos.

c) Secuencias de dirección URL denegadas.

d) Comandos.

El filtrado de solicitudes ha sustituido a la herramienta externa URLScan de versiones anteriores a la 7.5.

7.2.4 RESTRICCIONES

Las restricciones de direcciones IP y dominios, como su nombre indica, ofrece la opción de permitir o denegar a usuarios, grupos, redes, subredes, etc. el acceso al sitio.

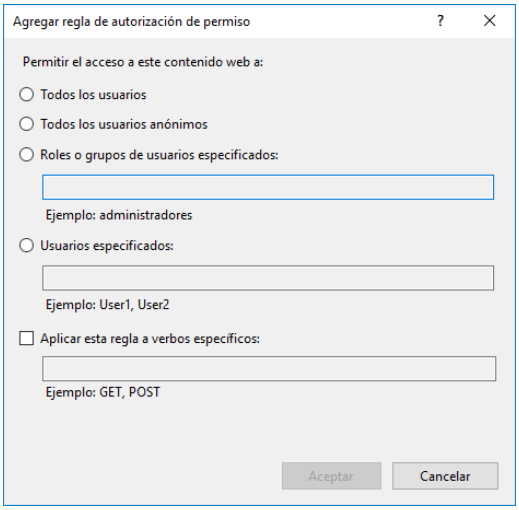
Se pueden crear entradas para los servidores web de IIS o para el servidor FTP.

Las restricciones operan sobre las versiones 4 y 6 de IP (IPv4 e IPv6), pero tenga en cuenta que en su instalación del servidor se ha podido deshabilitar la última.

Se pueden crear tantas entradas como se considere y se pueden ordenar para conseguir el efecto deseado, ya que un acceso será restringido o permitido según la línea que le afecte primero, por lo que el orden de prioridad es determinante para el funcionamiento.

Las restricciones de direcciones IP y dominios para el servidor web es un módulo instalable individual, mientras que para el caso de FTP se instala con el módulo del servidor.

Mientras no se crea ninguna entrada el servidor permitirá todos los accesos y el servicio del rol de restricciones estará inoperativo.



Para que se permita la opción de "Nombre de dominio" debe haber modificado antes el módulo con la opción "Modificar configuración de característica…".

También se puede instalar el módulo de "Restricciones de ISAPI y CGI" que dependen directamente de que se hayan instalado, a su vez, los módulos de ISAPI y CGI. Administra una lista de restricciones para programas ISAPI (.dll) o CGI (.exe). Cuando es ineludible instalar un servidor con programas ejecutables se considera que la vulnerabilidad del mismo aumenta en gran medida por lo que restringir su uso lo más posible es indispensable, de ahí la existencia de este nivel de seguridad.

7.2.5 PERMISOS

El nivel de permisos NTFS en ficheros y carpetas aumenta la administración de una forma considerable ya que exige un esfuerzo grande y grandes dotes de organización para evitar problemas de aperturas indiscriminadas o la imposibilidad de servir el recurso por falta de permisos adecuados.

Los permisos NTFS son atributos propios de los elementos que protegen. Este punto de partida ayuda a entender mejor la seguridad de ficheros en Windows. Las herramientas de administración de los permisos del sistema operativo ayudan facilitando las modificaciones en cadena, cuando así se quiere hacer, pero como último resultado es un permiso de un objeto.

Las autorizaciones, filtros o restricciones no pueden sustituir la falta de un permiso para el acceso a un determinado fichero. Se requiere un permiso para el acceso, la denegación o la ausencia de permiso para un usuario le imposibilitarán el acceso a dicho fichero. El permiso, el usuario, lo puede recibir de forma directa o por pertenencia a un grupo que lo reciba.

Existe la posibilidad de la representación del usuario, de esta forma no tenemos por qué conceder permisos a un usuario de forma predeterminada. Si, por ejemplo, el grupo de aplicaciones que está utilizando se ejecuta sobre una cuenta que tiene los permisos adecuados y se ha habilitado que represente a los usuarios.

Como para cualquier otro recurso, Microsoft recomienda la utilización del modo de asignación estándar: **Cuentas de usuarios → Grupos del dominio → Grupos locales → Permisos**. Este método evita las reescrituras constantes de permisos que hacen pesadas las tareas de mantenimiento.

Cuando los accesos son desde fuera del dominio la gestión del acceso por medio de permisos NTFS suele ser difícil y deficiente al no poder distinguir usuarios, por lo que se debería combinar con otros niveles de seguridad o no utilizarlo. Lo mismo se puede decir de la auditoría de objetos.

7.3 CERTIFICADOS

Los servidores seguros que utilizan cifrado SSL/TLS permiten que el intercambio de información entre ellos y los clientes no pueda ser capturado de forma directa y en todo caso hace que el ataque sea mucho más improbable y complejo que sin usar técnicas criptográficas.

IIS utiliza, de forma predeterminada, el repositorio de certificados del servidor Microsoft Server 2016, donde puede alojar certificados digitales que utilizará en las comunicaciones.

Los certificados pueden ser emitidos por el propio servidor IIS (autofirmado), por una autoridad certificadora (CA) dentro del bosque/dominio o por una CA pública (FNMT, Verisign, Chamberts of Commerce, etc.). Cada uno de ellos pensado para un ámbito más o menos concreto.

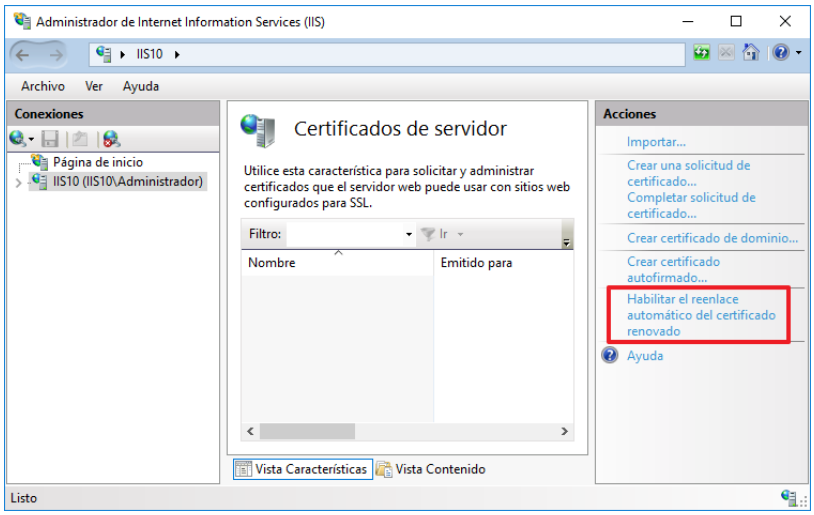
Los certificados autorfirmados se deben limitar a un uso en entornos de prueba o completamente cerrados y para acceso desde la LAN propia y con usuarios conocedores del entorno y que pueden confiar en un acceso sin entidad certificadora raíz conocida. En esta guía se han utilizado estos certificados para asegurar las comunicaciones con SSL. Su administración es la más sencilla y no requiere ninguna instalación adicional o compra de certificado externo.

Los certificados gestionados por el dominio requieren instalar una autoridad certificadora integrada con el Directorio activo, en un equipo servidor distinto al de IIS. La gestión es, de las tres opciones, la más compleja y con mayor carga administrativa. Como ventaja tienen la no limitación de emisión de certificados y la ausencia de coste en la emisión. Se debe utilizar esta opción para proteger comunicaciones en redes propias y con clientes del dominio o bosque propios.

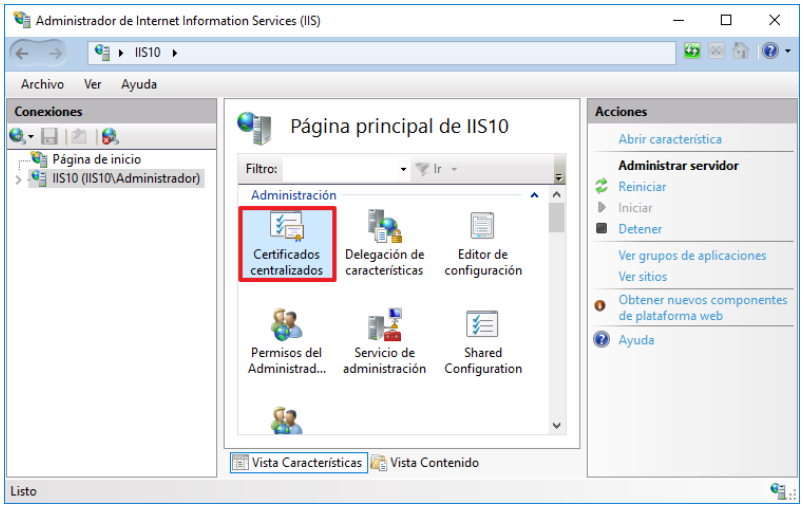
Los certificados emitidos por autoridades certificadoras de raíz públicas permiten asegurar sitios que están presentes en Internet y cuyos clientes solo tienen como única forma de comprobar la veracidad del sitio este certificado. La gestión es fácil y solo debe alojarse en el repositorio de certificados y darle uso, por contra tienen un coste para cada certificado que se solicite. En algunos casos es necesario alojar el certificado de la entidad raíz en los navegadores, si bien no es necesario en los principales proveedores de seguridad del mercado, en los que los navegadores de más uso ya los llevan integrados (no es el caso de la FNMT, que sí requiere dicha instalación).

La renovación de certificados cuando aún no han caducado suele ser una tarea fácil ya que se puede utilizar el certificado todavía válido como medio de certificar nuestra identidad y para cifrar las comunicaciones, sin embargo, cuando un certificado ha caducado se debe proceder a su sustitución por uno nuevo.

IIS 10 incorpora una nueva funcionalidad que permite volver a vincular un certificado renovado de forma automática. Para ello, en certificados de servidor, se debe "Habilitar el reenlace automático del certificado renovado".



Cuando un administrador dispone de múltiples servidores o sitios web puede reducir la carga de trabajo derivada de la gestión de certificados creando un repositorio central al que pueden acceder todos los equipos que compartan este medio de aseguramiento. Esta funcionalidad de IIS 10 se la conoce como "Certificados centralizados".



8. NUEVAS CARACTERISTICAS INTRODUCIDADAS EN IIS 10

IIS 10 es la última versión de Internet Information Services (IIS) que se incluye con Windows 10 y Windows Server 2016. Este apartado describe las nuevas funcionalidades de la nueva versión de IIS que va a ser desplegado y configurado sobre un sistema operativo servidor Windows Server 2016.

8.1 SEGURIDAD DE TRASNPORTE HTTPS /2 Y HSTS

8.1.1 DESCRIPCIÓN HTTPS /2

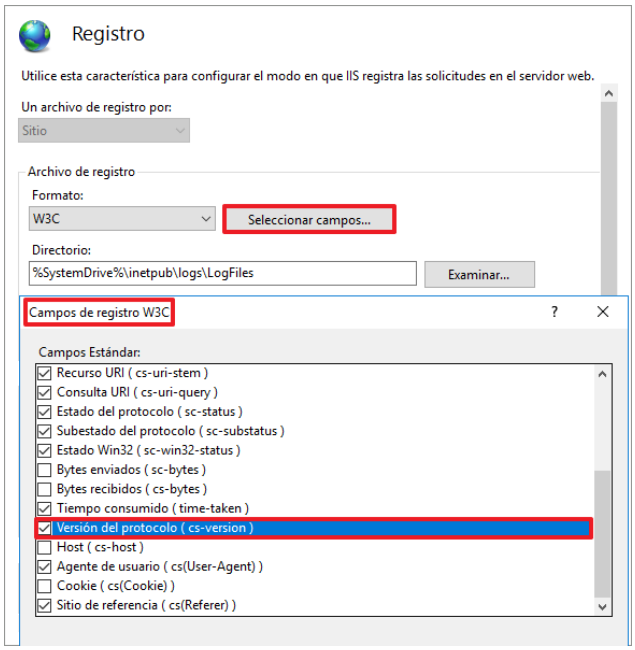
IIS 10 incorpora a su amplio abanico de características la compatibilidad con el protocolo HTTP / 2, que permite numerosos beneficios sobre HTTP / 1.1 y da como consecuencia una reutilización eficiente en el tiempo de envío y recepción de datos (latencia).

El soporte HTTP / 2 ha sido agregado a Windows Server 2016 como parte del controlador de dispositivo en modo kernel, HTTP.sys, y todos sus sitios web pueden beneficiarse de esta mejora.

Es importante indicar que las últimas versiones de los navegadores web más modernos son compatibles con HTTP / 2 sobre TLS, por lo que es posible que este protocolo ya se esté utilizando.

Las conexiones entre cliente y servidor por tanto siempre que esta sea compatible será realizada mediante HTTP / 2, mientras que si este condicionante no se cumple IIS pasará a retroceder a la versión HTTP / 1.1.

Con el fin de determinar si es posible realizar una conexión mediante el protocolo citado, IIS 10 ofrece una configuración que permite determinar el protocolo utilizado. Para activar esta configuración basta con acceder al apartado “Registro” y habilitar el campo “Versión de protocolo”. De este modo se registrarán las conexiones realizadas y con qué tipo de protocolo.



También es importante aclarar que la autenticación propia de Windows (NETLM, Kerberos) no está soportado por esta característica por lo que IIS hará uso de HTTP / 1.1.

8.1.2 DESCRIPCION HSTS

HSTS es una mejora de seguridad opcional que aplica HTTPS y reduce significativamente la capacidad de los ataques tipo “man-in-the-middle” para obstaculizar solicitudes y respuestas entre servidores y clientes.

HSTS implanta el uso de HTTPS a través de una política que requiere soporte tanto de los servidores web como de los navegadores. Un host web habilitado para HSTS puede incluir un encabezado de respuesta HTTP especial "Strict-Transport-Security" (STS) junto con una directiva de "máximo de edad" en una respuesta HTTPS para solicitar al navegador que use HTTPS para una mayor comunicación.

Nota: Para más información consulte el siguiente enlace.
https://docs.microsoft.com/es-es/iis/get-started/whats-new-in-iis-10-version-1709/iis-10-version-1709-hsts